SICHERHEITSREPORT ENTSCHEIDER 2016

ERGEBNISSE EINER REPRÄSENTATIVEN UMFRAGE

ERLEBEN, WAS VERBINDET.

INHALT

STICHPROBE
619 Personen, davon 512 Top-Entscheider aus großen (239) und mittleren (273) Unternehmen sowie107 Politiker (EU-Parlamentarier (9), Bundestagsabgeordnete (41), Landtagsabgeordnete (57)

METHODE
Computergestützte telefonische Interviews (CATI)

BEFRAGUNGSZEITRAUM
29. August bis 7. Oktober 2016

ANZAHL DER EINGESETZTEN INTERVIEWER
14 geschulte Telefoninterviewer

AUSWAHLMETHODE
Geschichtete Zufallsauswahl

VORBEMERKUNG

Bereits im sechsten Jahr in Folge hat das INSTITUT FÜR DEMOSKOPIE ALLENSBACH im Auftrag von T-SYSTEMS und in Kooperation mit dem CENTRUM FÜR STRATEGIE UND HÖHERE FÜHRUNG Top-Entscheider aus Politik und Wirtschaft zu ihren allgemeinen Risikoeinschätzungen sowie zu ausgewählten Themen aus dem Bereich „Cyber Security“ befragt. Die inzwischen sechste Welle des Cyber Security Reports erlaubt damit für zahlreiche Fragen eine Analyse in Bezug auf die Entwicklung der Risikowahrnehmungen im Zeitverlauf. Die Studie zeigt, dass Cyber- und Datenrisiken aus Sicht der Entscheider in Politik und Wirtschaft nach wie vor ein großes Gefahrenpotenzial für Deutschland, seine Bürger und die Unternehmen bergen.

Neben den Trendfortschreibungen zu den Einschätzungen von Risiken aus verschiedenen Lebensbereichen, dem Stellenwert der IT-Sicherheit im jeweils eigenen Unternehmen, der Bedrohung durch IT-Angriffe und der Bewertung der staatlichen Fachkompetenz im Bereich IT-Sicherheit widmet sich die vorliegende Studie vier Cyber-Themen ausführlicher. Ergänzend zu den Fragen der individuellen Gefährdung im Zusammenhang mit der Cyber-Sicherheit von Smartphones, der Verschlüsselung von E-Mails und der Nutzung und Sicherheitsbewertung von „Cloud Computing“ wurden auch Einschätzungen zu möglichen Cyber-Attacken auf Deutschland erhoben.

Die Studie stützt sich auf insgesamt 619 telefonische Interviews, die zwischen Ende August und Anfang Oktober 2016 durchgeführt wurden. Daran teilgenommen hat ein repräsentativer Querschnitt von Politikern sowie Top-Führungskräften aus mittleren und großen Unternehmen. Aus dem politischen Bereich wurden 107 Abgeordnete aus dem Bundestag, den Landtagen sowie deutsche Abgeordnete des Europaparlaments befragt. Als Entscheider aus der Wirtschaft wurden insgesamt 512 Führungskräfte interviewt, darunter 239 Führungskräfte aus großen und 273 Führungskräfte aus mittleren Unternehmen. Dieser Abgrenzung nach Unternehmensgröße liegt die Definition der EU-Kommission zugrunde, gemäß welcher Unternehmen mit 250 und mehr Beschäftigten und/oder mehr als 50 Mio. Euro Jahresumsatz als große Unternehmen gelten. Mittlere Unternehmen sind demgegenüber Unternehmen, 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 nur gut 2 Prozent aller Unternehmen in Deutschland, erwirtschaften aber rund 80 Prozent aller umsatzsteuerpflichtigen Waren und Dienstleistungen und beschäftigen etwa zwei Drittel aller sozialversicherungspflichtigen Arbeitnehmer in Deutschland.

Aber nicht nur im Hinblick auf die Größe der Unternehmen konnte erneut eine hochkarätige Stichprobe realisiert werden. Von den befragten Entscheidern aus der Wirtschaft gehören gut zwei Drittel der ersten Führungsebene ihres Unternehmens an (Vorstände, Geschäftsführer, Inhaber). Ein weiteres knappes Drittel bekleidet z. B. als Bereichsleiter in einem Großunternehmen ebenfalls eine gehobene Position im eigenen Unternehmen.

Die wichtigsten Ergebnisse der Befragung sind im vorliegenden Bericht zusammengefasst und grafisch dargestellt.

INSTITUT FÜR DEMOSKOPIE ALLENSBACH
Allensbach am Bodensee,
am 31. Oktober 2016

GESELLSCHAFTLICHE RISIKEN: AUS SICHT VON POLITIKERN UND WIRTSCHAFTSFÜHRERN BERGEN IT- UND DATENRISIKEN DAS GRÖSSTE GEFAHRENPOTENZIAL

Aus Sicht von Top-Entscheidern aus Politik und Wirtschaft stellen Cyber-Gefahren und mögliche Datenschutzverletzungen unter 20 Risiken aus allen Lebensbereichen die größte Bedrohung für die Bevölkerung in Deutschland dar. Unter den sieben Risiken, die am häufigsten als große Gefahr für die Menschen in Deutschland genannt werden, finden sich fünf Risiken, die mit IT- und Datensicherheit zusammenhängen, darunter die „Top 3" der Nennungen: 72 Prozent der Entscheider nehmen Computerviren als großes Risiko für die Menschen in Deutschland wahr, 70 Prozent möglichen Datenbetrug im Internet, 64 Prozent den Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken, 52 Prozent den Missbrauch von persönlichen Daten durch Unternehmen. Weniger Gefahrenpotenzial birgt aus Sicht der Entscheider dagegen die staatliche Überwachung der Bürger, insbesondere der Internet- oder Telefonverbindungen: 41 Prozent der Entscheider sehen in der Überwachung deutscher Bürger durch ausländische Staaten ein großes Risiko für die Bevölkerung, 16 Prozent in der Überwachung durch den deutschen Staat. Daneben sehen 57 Prozent der Führungskräfte ein großes Risiko darin, dass man durch die Digitalisierung von Computern abhängig ist. Dies ist zwar kein Risiko der IT- oder Datensicherheit im engeren Sinne, aber ein Risiko, das mit der zunehmenden Digitalisierung aller Lebensbereiche einhergeht.

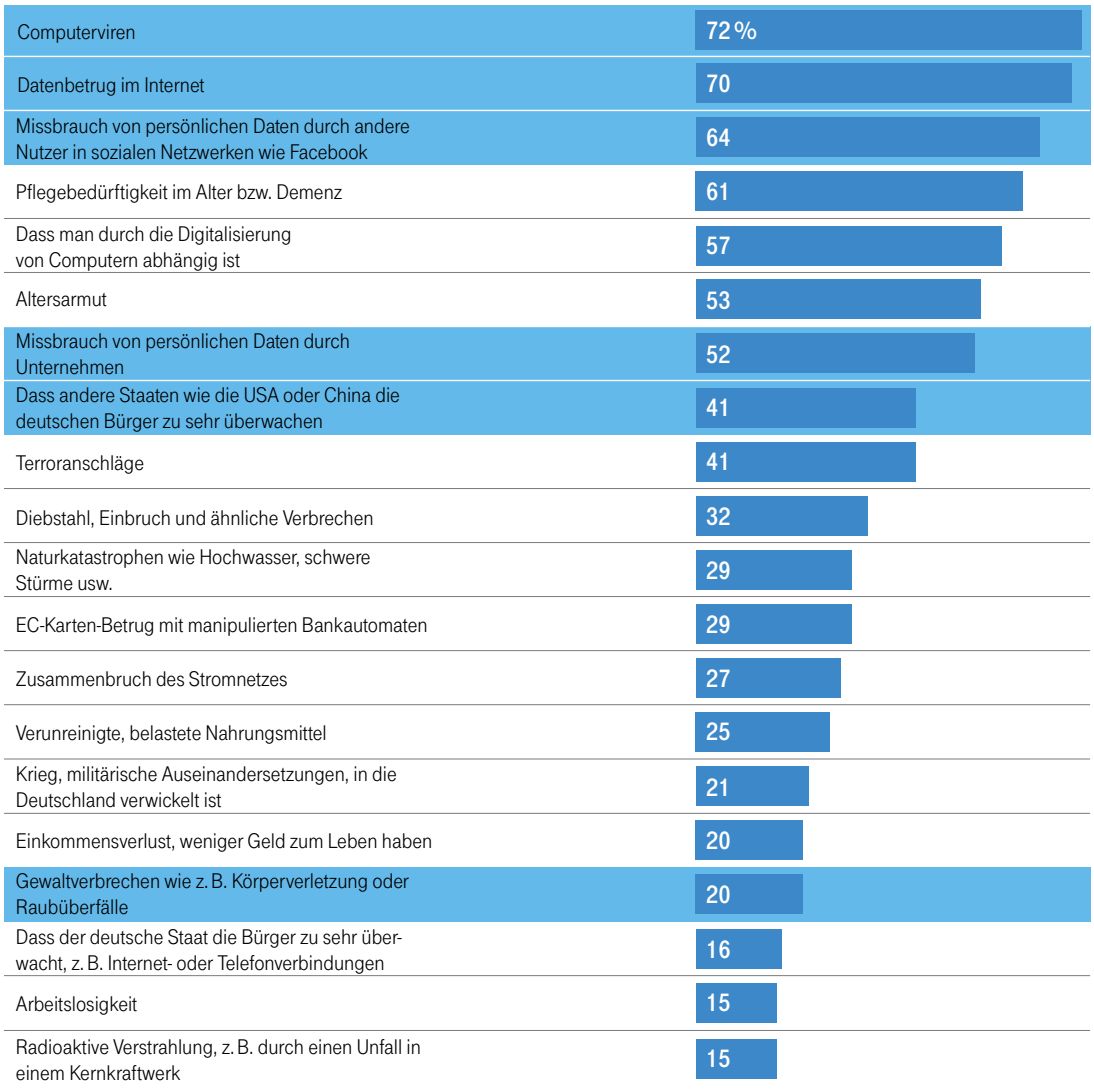
Im Vergleich zu diesen IT- und Datenrisiken werden von Abgeordneten und Wirtschaftsführern nur Risiken im Kontext von Alter und demografischem Wandel als ähnlich bedeutsam eingestuft: So sehen 61 Prozent der Entscheider die Pflegebedürftigkeit im Alter, 53 Prozent mögliche Altersarmut als großes Risiko für die Bevölkerung.

Abgesehen von der Gefahr von Terroranschlägen, die von 41 Prozent der Entscheider als großes Risiko für die Bevölkerung wahrgenommen werden, folgen andere Risiken erst mit deutlichem Abstand: Diebstahl, Einbruch und ähnliche Straftaten sind nach Einschätzung von 32 Prozent der Entscheider ein großes Risiko, Naturkatastrophen und EC-Karten-Betrug folgen mit jeweils 29 Prozent. Insbesondere materielle Risiken wie Einkommensverlust oder Arbeitslosigkeit spielen mit 20 bzw. 15 Prozent nur eine untergeordnete Rolle (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 –

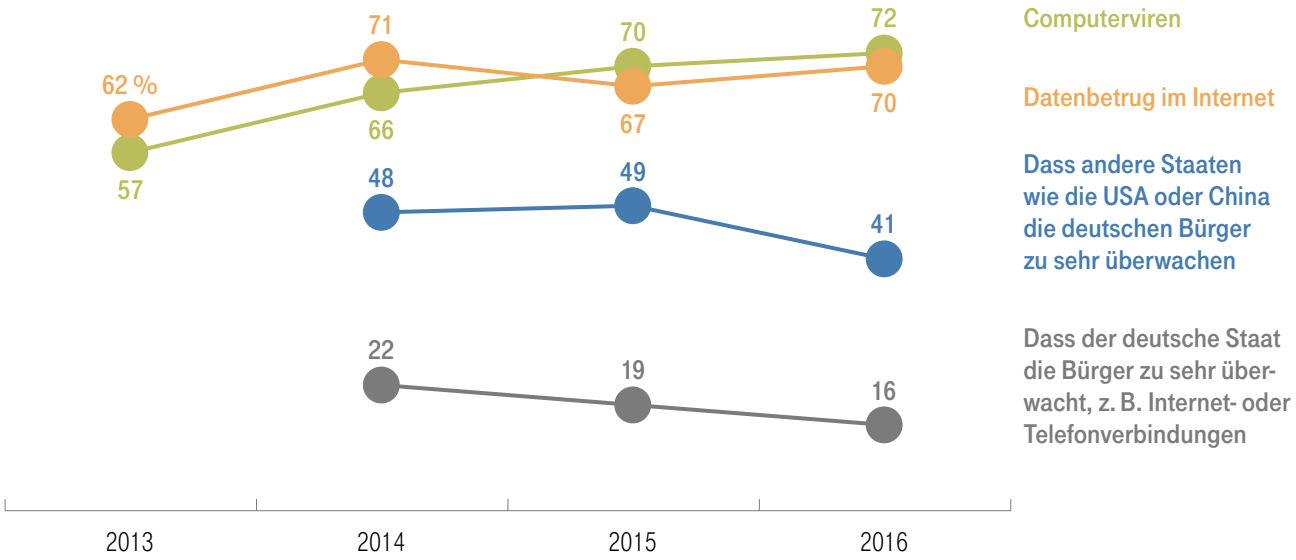


Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 1

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 7251 (September 2016)

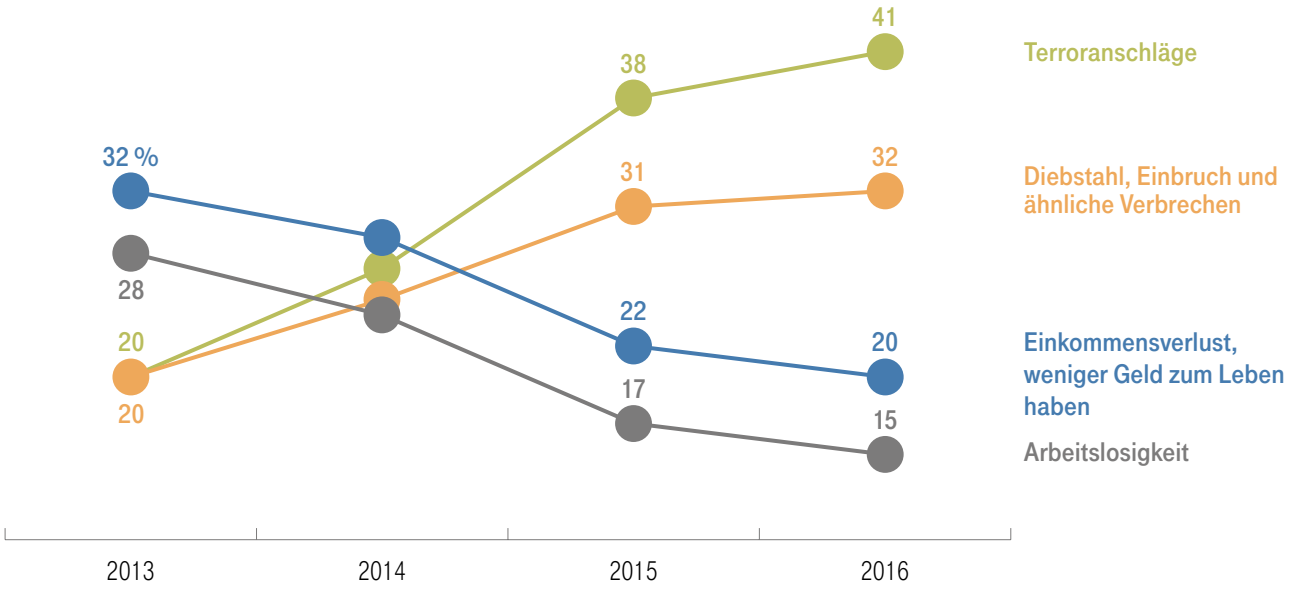
Schaubild 2

Der Anteil der Entscheider, der große Risiken durch Computerviren sieht, ist in den letzten drei Jahren von 57 Prozent auf aktuell 72 Prozent deutlich angestiegen. Die Gefahr durch Datenbetrug im Internet wird seit zwei Jahren von stabil etwa 70 Prozent als hoch eingeschätzt.

Dagegen sieht derzeit im Vergleich zu den letzten beiden Jahren ein deutlich kleinerer Anteil der Entscheider große Risiken für Bürger durch die Überwachung durch andere Staaten wie die USA oder China. Der Anteil ist von 49 Prozent im letzten Jahr auf 41 Prozent zurückgegangen. Und auch der Anteil derer, die Gefahren durch die Überwachung durch den deutschen Staat sehen, ist weiter rückläufig (Schaubild 2).

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 –



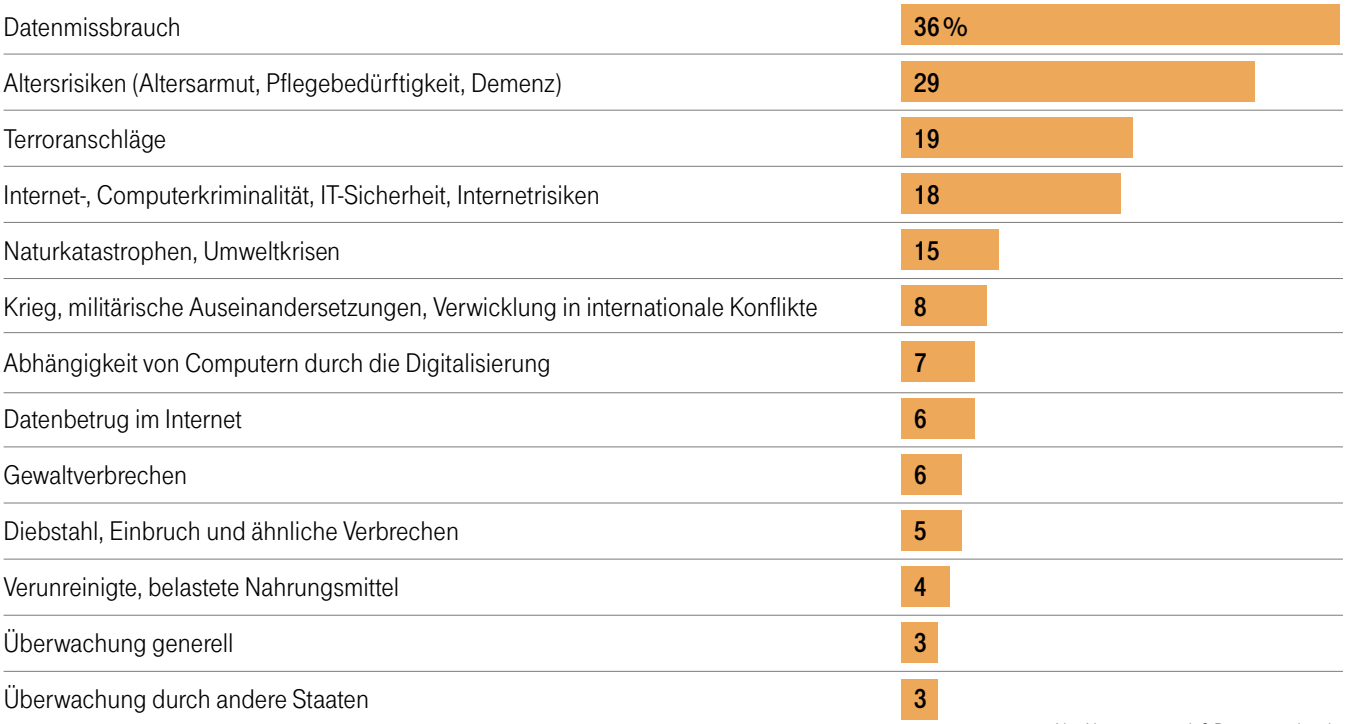
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7251 (September 2016)

Schaubild 3

Materielle Risiken haben vor dem Hintergrund der guten gesamtwirtschaftlichen Entwicklung erneut an Bedeutung verloren. So sehen aktuell nur 15 Prozent der Entscheider Arbeitslosigkeit als großes Risiko für die Bevölkerung in Deutschland – vor drei Jahren waren es noch 28 Prozent. Demgegenüber sind die wahrgenommenen Gefahrenpotenziale von Diebstählen, Einbrüchen und ähnlichen Verbrechen ebenso wie die von Terroranschlägen seit 2013 kontinuierlich gestiegen. Rund jeder dritte Entscheider sieht inzwischen Diebstahls- und Einbruchsdelikte als großes gesellschaftliches Risiko, 2013 waren es lediglich 20 Prozent. Mit Blick auf die Gefährdung durch Terroranschläge hat sich der Anteil derer, die hier ein großes Risiko für die Menschen in unserem Land sehen, in den letzten Jahren sogar mehr als verdoppelt. 2013 nahmen 20 Prozent der Entscheider Terroranschläge als großes Risiko wahr, aktuell sind es 41 Prozent (Schaubild 3).

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)



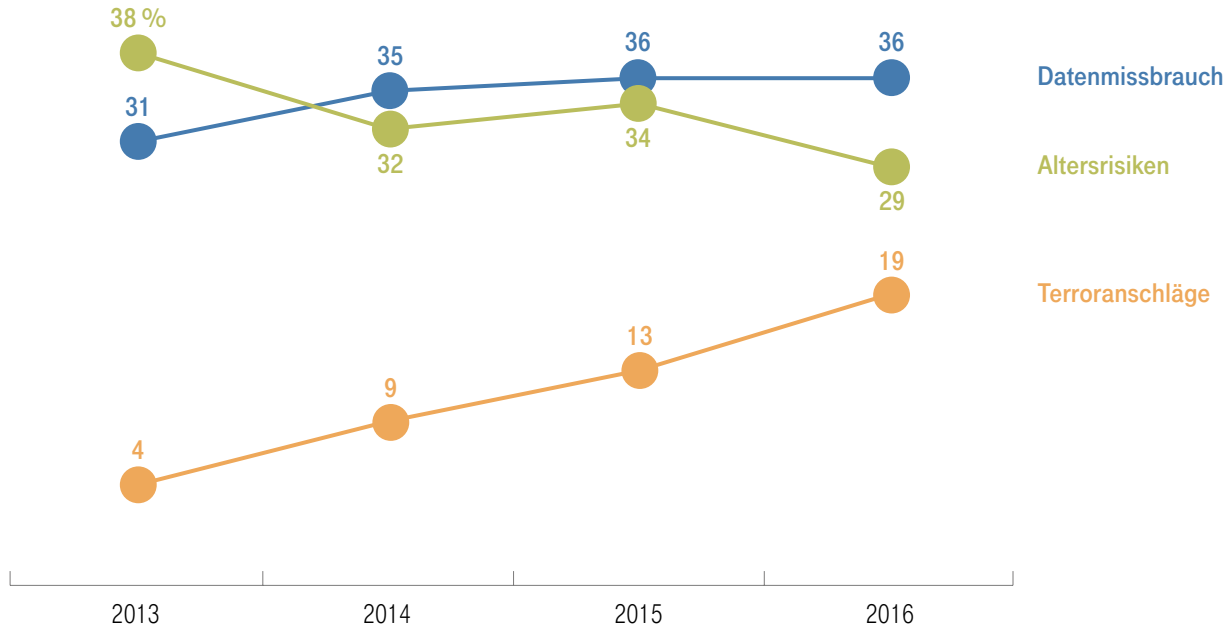
Nur Nennungen mit 3 Prozent und mehr

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 4

Für die Zukunft erwarten die Entscheider aus Politik und Wirtschaft vor allem eine Zunahme von Cyber-Risiken, von Altersrisiken sowie des Risikos von Terroranschlägen. Da die Einschätzung zur zukünftigen Risikoentwicklung offen erfragt wurde, also ohne dass mögliche Antworten vorgegeben wurden, ist ein Vergleich der absoluten Werte mit der derzeitigen Risikobewertung zwar nicht möglich. Aber bemerkenswert häufig benennen Politiker und Führungskräfte aus mittleren und großen Unternehmen Cyber- und Datenrisiken spontan als wichtige Zukunftsgefahren. 36 Prozent verweisen auf den Datenmissbrauch als wachsende Gefahrenquelle, 18 Prozent auf Internet- und Computerkriminalität sowie die IT-Sicherheit generell, 6 Prozent rechnen mit einer besonders starken Zunahme von Datenbetrug im Internet. Dass mindestens eines dieser drei Risiken künftig stark zunehmen wird, davon gehen 55 Prozent der Entscheider aus. Damit werden aus Sicht von Abgeordneten und Führungskräften in der Wirtschaft IT- und Datenrisiken künftig insbesondere stärker zunehmen als Altersrisiken wie Altersarmut und Pflegebedürftigkeit. Eine deutliche Zunahme dieser Risiken erwarten 29 Prozent der Entscheider (Schaubild 4).

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



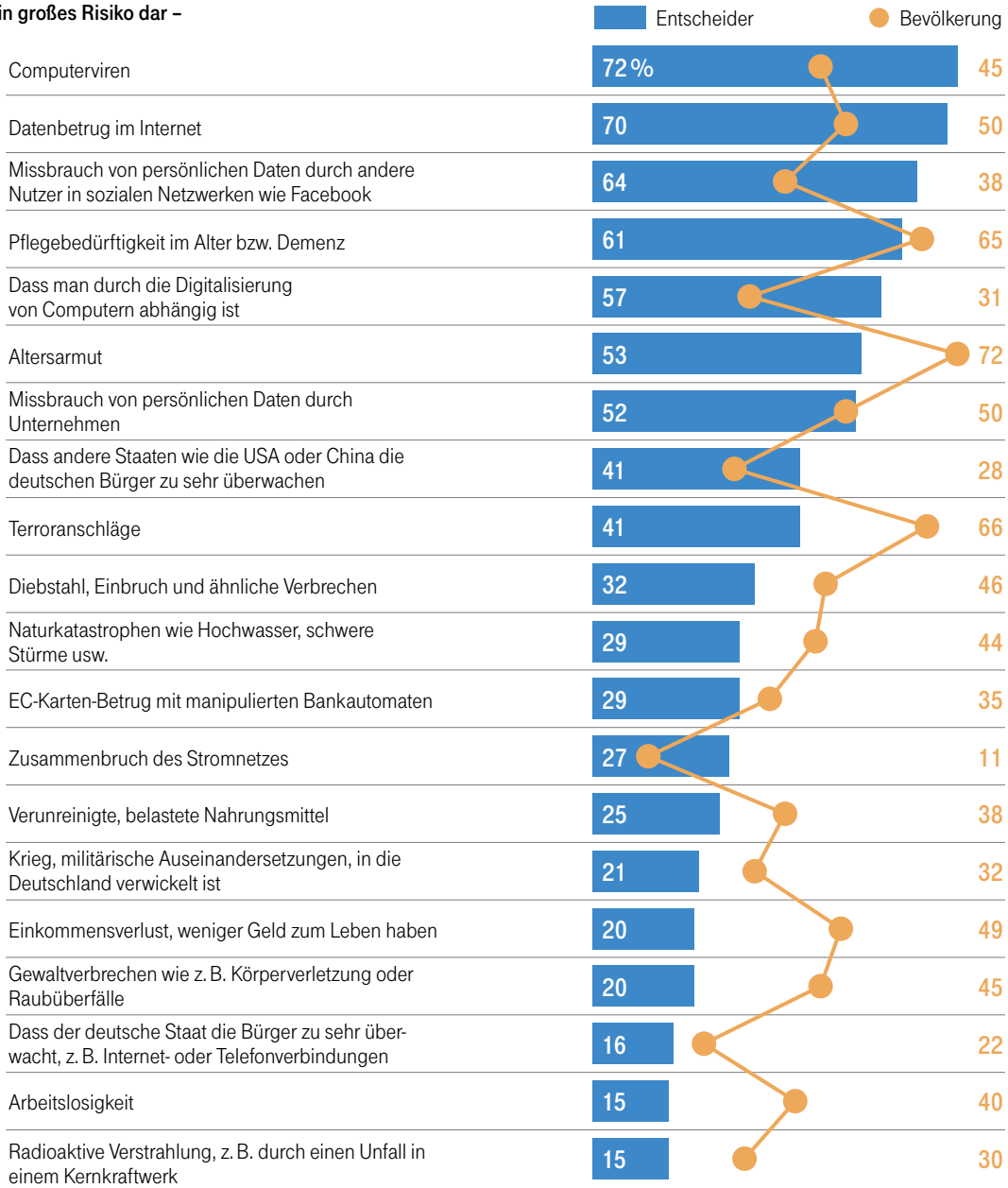
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7251 (September 2016)

Schaubild 5

Die Veränderung der Erwartungen zu künftigen Risikoentwicklungen in den letzten Jahren bestätigt die zuvor beschriebenen Trends. Im Vergleich zu den Vorjahren zeigt sich der Anteil der Entscheider, die eine starke Zunahme von Risiken durch Datenmissbrauch sehen, stabil auf hohem Niveau. Der Anteil derer, die eine deutliche Zunahme von Altersrisiken erwarten, ist demgegenüber von 38 Prozent 2013 auf aktuell 29 Prozent unübersehbar zurückgegangen. Umgekehrt ist der Anteil derer, die eine deutliche Zunahme des Risikos von Terroranschlägen befürchten, in den vergangenen drei Jahren kontinuierlich gestiegen: von 4 Prozent auf derzeit 19 Prozent (Schaubild 5).

RISIKOWAHRNEHMUNG VON BEVÖLKERUNG UND ENTSCHEIDERN IM VERGLEICH

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



Basis: Bundesrepublik Deutschland, Bevölkerung ab 16 Jahren, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 11059 (August 2016), 7251 (September 2016)

Schaubild 6

Die Einschätzungen der verschiedenen Risikopotenziale durch die Entscheider aus Wirtschaft und Politik unterscheiden sich zum Teil erheblich von den Risikoeinschätzungen der Bevölkerung. Insbesondere messen die Führungskräfte den Cyber- und Datenrisiken mehr Bedeutung bei als die Bevölkerung. Die Bevölkerung sieht hingegen vor allem bei materiellen Risiken, bei Terroranschlägen und bei der klassischen Kriminalität größere Risiken.

So stellen Computerviren für 72 Prozent der Entscheider, aber nur für 45 Prozent der Bevölkerung ein großes gesellschaftliches Risiko dar. Beim Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzen sehen rund zwei Drittel der Entscheider ein großes Risiko für die Menschen in Deutschland, aber lediglich 38 Prozent der Bevölkerung. Und auch den Umstand, dass die Menschen durch die Digitalisierung von Computern abhängig sind, sieht eine deutliche Mehrheit der Entscheider, aber nur ein knappes Drittel der Bevölkerung als große Gefahr.

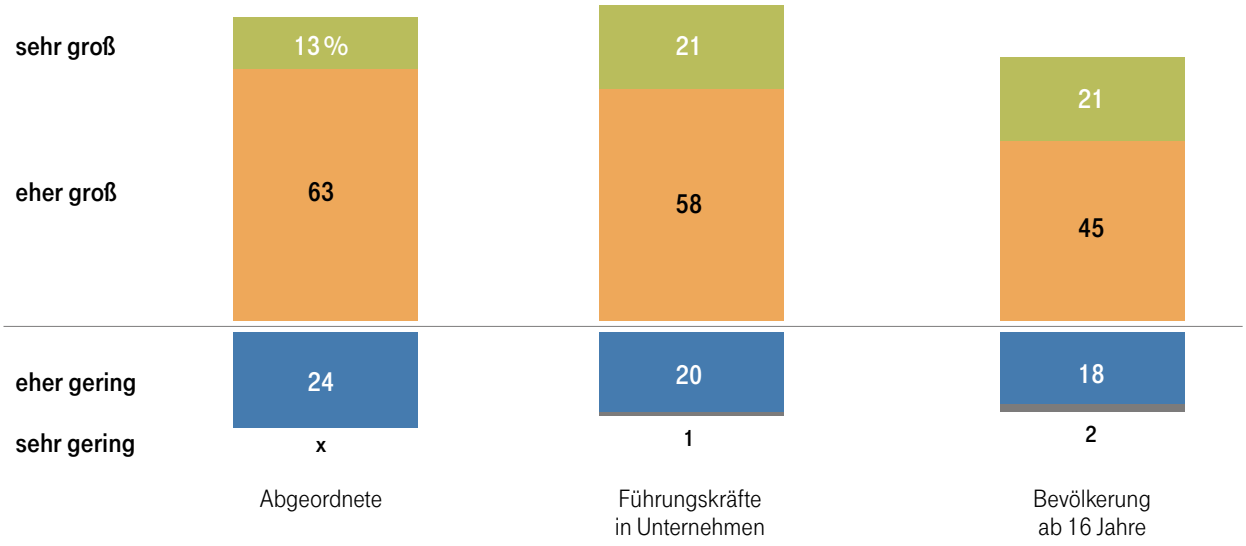
Umgekehrt halten 49 Prozent der Bevölkerung, aber nur 20 Prozent der Entscheider mögliche Einkommensverluste für ein großes Risiko. Ähnliches gilt für die Risiken von Arbeitslosigkeit (Bevölkerung: 40 Prozent, Entscheider: 15 Prozent) oder Altersarmut (Bevölkerung: 72 Prozent, Entscheider: 53 Prozent). Das Risiko für die Menschen durch Terroranschläge halten zwei Drittel der Bevölkerung für groß, von den Entscheidern „nur“ 41 Prozent. Und auch die Risiken, die von Gewaltverbrechen oder Diebstählen ausgehen, werden von der Bevölkerung im Vergleich zu den politischen und wirtschaftlichen Entscheidern deutlich häufiger als groß eingeschätzt (Schaubild 6).

CYBER-ANGRIFFE AUF DEUTSCHLAND: ENTSCHEIDER SEHEN GROSSE GEFAHREN DURCH ANGRIFFE AUF DIE INFRASTRUKTUR

ENTSCHEIDER UND BEVÖLKERUNG SIND SICH EINIG: DIE GEFAHR EINES CYBER-ANGRIFFS AUF DEUTSCHLAND IST EHER GROSS

Frage: „Für wie groß halten Sie die Gefahr, dass die Sicherheit in Deutschland durch einen Cyber-Angriff auf staatliche Stellen oder auf die Infrastruktur, z. B. auf die Energieversorgung, gefährdet wird?“

Die Gefahr, dass die Sicherheit in Deutschland durch einen Cyber-Angriff gefährdet wird, ist –



x = unter 0,5 Prozent
Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Bevölkerung ab 16 Jahren, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 11059 (August 2016), 7251 (September 2016)

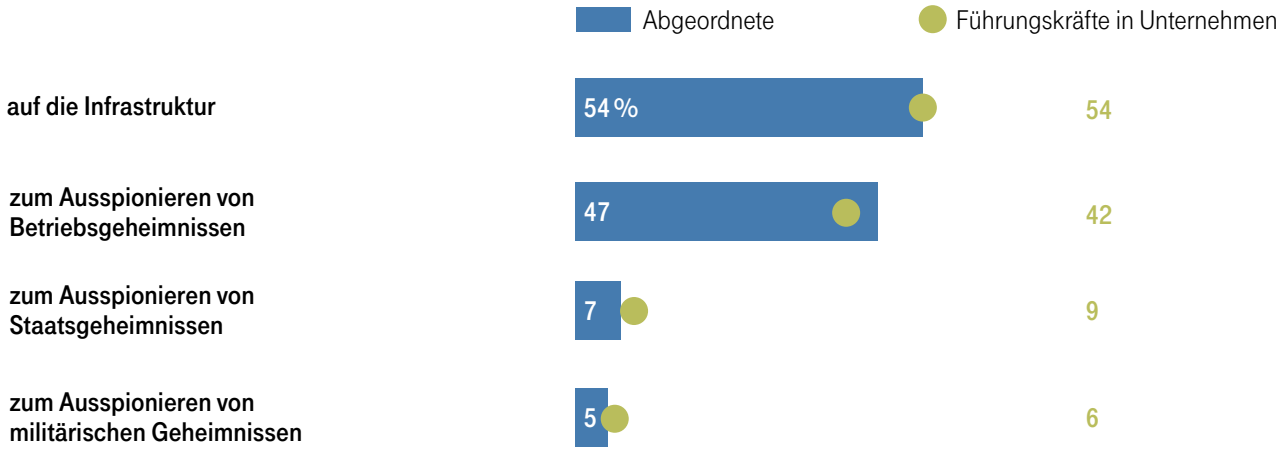
Schaubild 7

Die Gefahr, dass die Sicherheit in Deutschland durch Cyber-Angriffe gefährdet wird, hält eine deutliche Mehrheit der Entscheider aus Politik und Wirtschaft für groß: Von den Abgeordneten sind 13 Prozent davon überzeugt, dass die Gefahr, die von einem möglichen Cyber-Angriff auf staatliche Stellen oder Infrastruktureinrichtungen in Deutschland ausgeht, sehr groß ist, weitere 63 Prozent halten sie für eher groß. Unter den Führungskräften mittlerer und großer Unternehmen urteilen 21 Prozent bzw. 58 Prozent so. Auch wenn sich die Entscheider in dieser Frage besorgter zeigen als die Bevölkerung, ist die Urteilstendenz doch ganz ähnlich: Auch in der Bevölkerung halten zwei Drittel die Gefahr, dass die Sicherheit in Deutschland durch einen Cyber-Angriff gefährdet wird, für sehr oder eher groß (Schaubild 7).

GRÖSSTE GEFAHR DURCH EINEN ANGRIFF AUF DIE INFRASTRUKTUR UND BETRIEBSSPIONAGE

Frage: „Was würden Sie sagen, von welcher Art Cyber-Attacke geht für Deutschland die größte Gefahr aus: von Cyber-Attacken zum Ausspionieren von militärischen Geheimnissen oder von Staatsgeheimnissen oder von Betriebsgeheimnissen oder von Cyber-Attacken auf die Infrastruktur oder wovon sonst?“

Die größte Gefahr geht aus von Cyber-Attacken –
(Mehrfachangaben möglich)

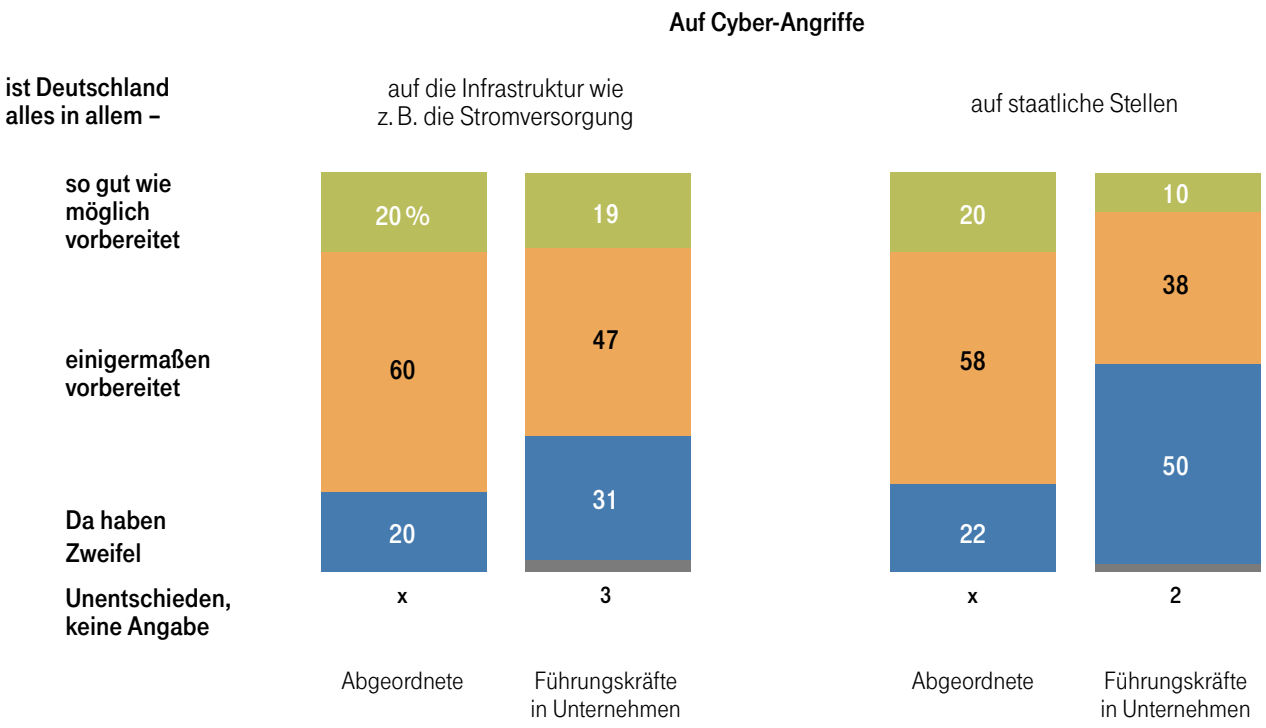


Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 8

Sowohl Abgeordnete als auch Führungskräfte aus der Wirtschaft sehen dabei die größte Gefahr von Cyber-Attacken auf Infrastruktureinrichtungen wie z. B. die Energieversorgung ausgehen. Jeweils 54 Prozent geben dies zu Protokoll. Nicht viel weniger häufig sehen sowohl Abgeordnete als auch Wirtschaftsführer mit die größten Gefahren für Deutschland in Cyber-Angriffen zur Betriebsspionage. In Cyber-Attacken zum Ausspionieren von Staatsgeheimnissen oder militärischen Geheimnissen sehen dagegen nur jeweils deutlich kleinere Anteile der Entscheider die größten Gefahrenpotenziale für Deutschland (Schaubild 8).

NUR EINE MINDERHEIT DER ENTSCHEIDER AUS POLITIK UND WIRTSCHAFT IST ÜBERZEUGT, DASS DEUTSCHLAND SO GUT WIE MÖGLICH AUF CYBER-ANGRIFFE VORBEREITET IST



x = unter 0,5 Prozent

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 9

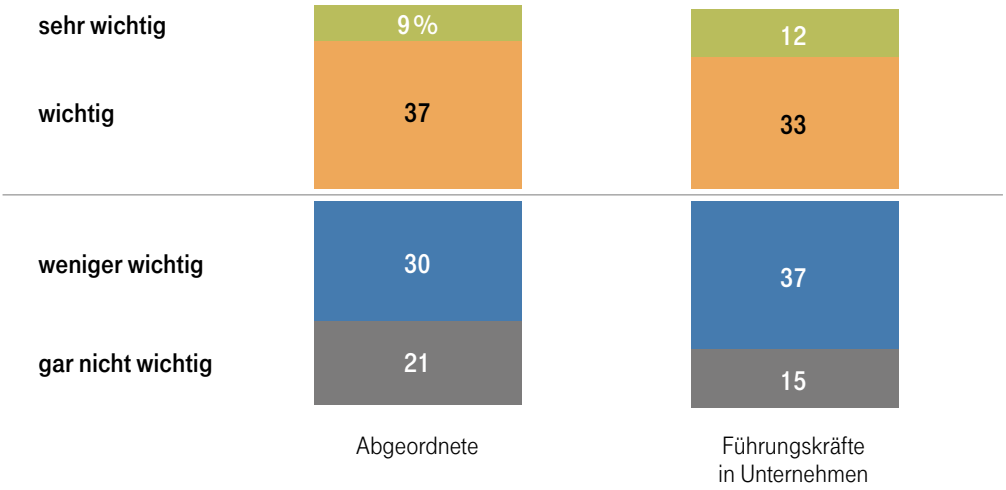
Nur eine Minderheit der Entscheider sieht Deutschland so gut wie möglich auf Cyber-Angriffe von außen vorbereitet. Dabei zeigen sich Wirtschaftsführer noch skeptischer als Politiker. Im Hinblick auf mögliche Cyber-Attacken auf die Infrastruktur wie beispielsweise die Energieversorgung hält nur jeweils rund ein Fünftel der Abgeordneten bzw. der Führungskräfte aus der Wirtschaft Deutschland für bestmöglich vorbereitet, ein knappes Drittel der Wirtschaftsführer zweifelt dagegen sogar daran, dass Deutschland hier auch nur einigermaßen vorbereitet ist.

Wenn es um einen Cyber-Angriff auf staatliche Stellen geht, urteilen vor allem Führungskräfte aus der Wirtschaft noch pessimistischer. Nur jeder Zehnte sieht Deutschland so gut wie möglich vorbereitet, die Hälfte geht davon aus, dass Deutschland darauf nicht einmal einigermaßen vorbereitet ist. Abgeordnete schätzen die Lage an dieser Stelle nicht ganz so negativ ein wie die Wirtschaftsführer, aber auch nicht positiver als im Hinblick auf mögliche Angriffe auf die Infrastruktur (Schaubild 9).

GESPALTENES MEINUNGSBILD ZUR BEDEUTUNG EIGENER CYBER-SPIONAGE

Frage: „Wie wichtig finden Sie es, dass auch der deutsche Staat versucht, in Computernetzwerke im Ausland einzudringen, um sich Informationen zu beschaffen?“

Das finden –



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 11059 (August 2016), 7251 (September 2016)

Schaubild 10

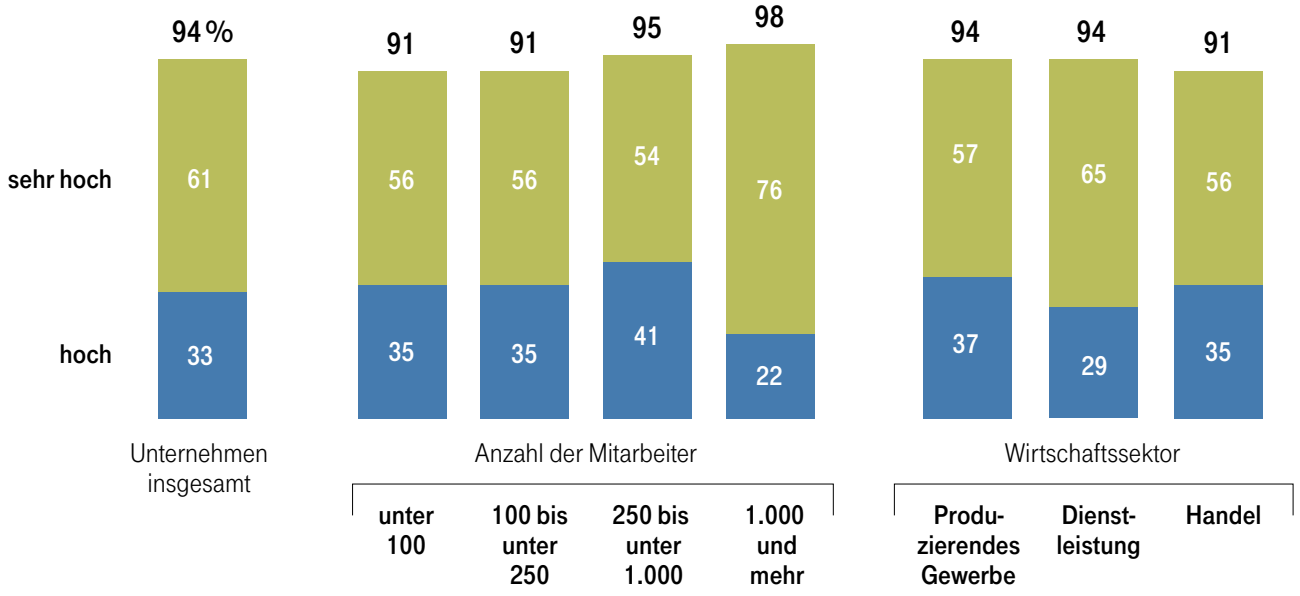
Wenn es darum geht, wie wichtig es ist, dass der deutsche Staat seinerseits in ausländische Netze eindringt, um Informationen zu beschaffen, ist das Meinungsbild der politischen und wirtschaftlichen Verantwortungsträger gespalten. In beiden Gruppen stehen jeweils rund 45 Prozent, die das für wichtig oder sehr wichtig halten, jeweils rund 50 Prozent gegenüber, die das ausdrücklich weniger wichtig oder gar nicht wichtig finden (Schaubild 10).

HOHER STELLENWERT VON IT-SICHERHEIT IN DEUTSCHEN UNTERNEHMEN, IT-ANGRIFFE UND WAHRGENOMMENES SCHADENSRISIKO NEHMEN DEUTLICH ZU

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?“

Stellenwert der IT-Sicherheit im Unternehmen ist –



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

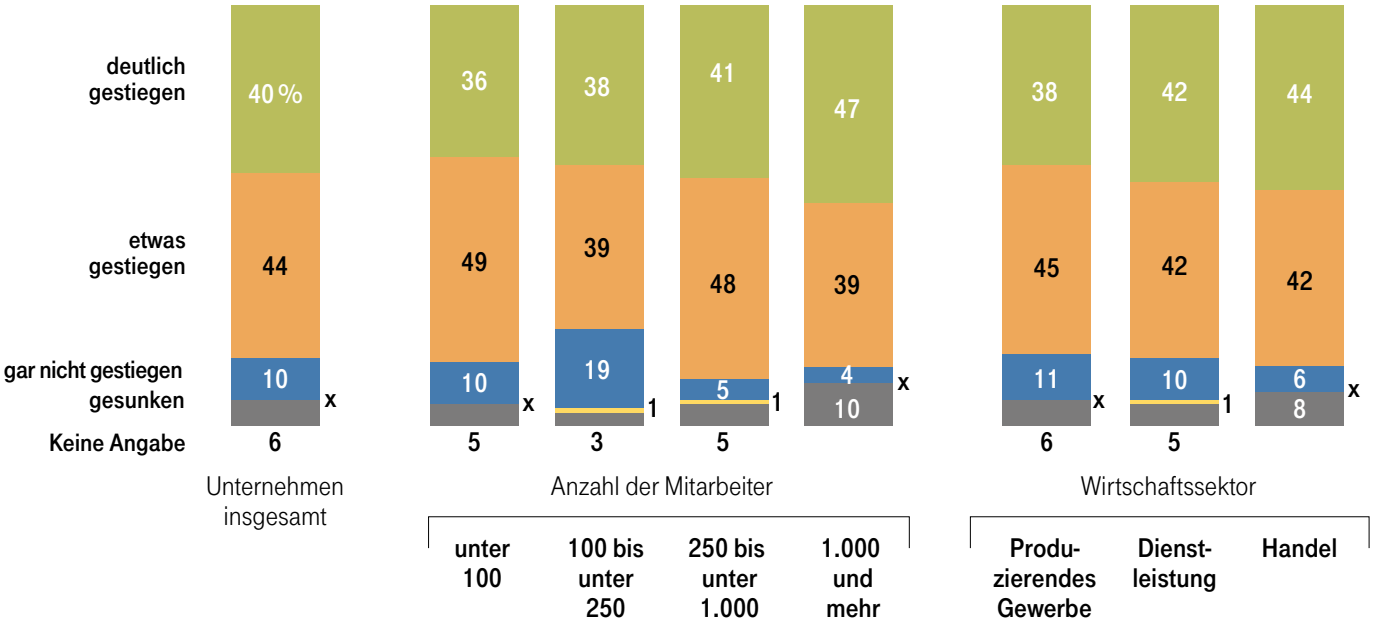
Schaubild 11

Die mittleren und großen Unternehmen in Deutschland messen der IT-Sicherheit eine große Bedeutung bei: 94 Prozent der Führungskräfte geben zu Protokoll, dass die IT-Sicherheit in ihrem Unternehmen einen hohen oder sogar sehr hohen Stellenwert hat. In sehr großen Unternehmen hat IT-Sicherheit dabei eine noch ausgeprägtere Bedeutung. Während Unternehmen mit weniger als 1.000 Mitarbeitern den Stellenwert der IT-Sicherheit zu gut 50 Prozent als sehr hoch veranschlagen, sind es in Unternehmen mit 1.000 und mehr Mitarbeitern 76 Prozent (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

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen

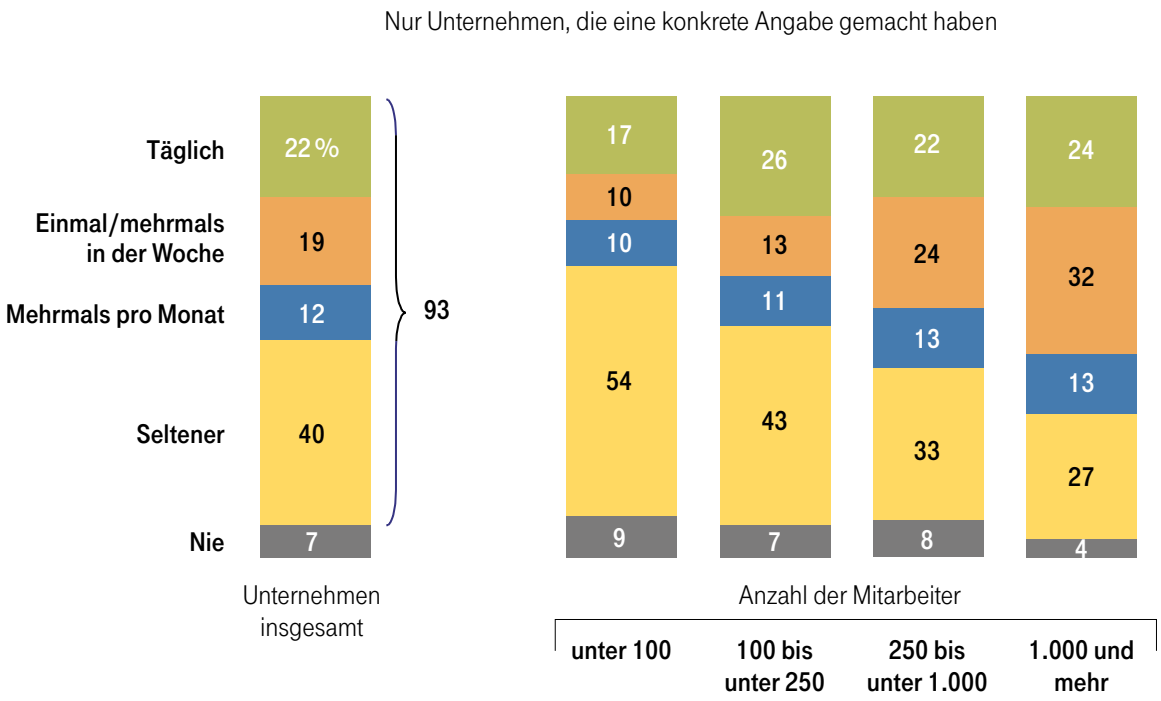
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 12

Der hohe Stellenwert, welcher der IT-Sicherheit beigemessen wird, schlägt sich in entsprechenden Investitionen nieder. In 40 Prozent der Unternehmen sind die Ausgaben für die IT-Sicherheit zum Schutz vor Hackerangriffen deutlich gestiegen, in weiteren 44 Prozent etwas gestiegen. Die Ausgabensteigerung in diesem Bereich ist in den verschiedenen Wirtschaftssektoren dabei sehr ähnlich. Eher noch spielt die Unternehmensgröße hier eine Rolle: Der Anteil der Unternehmen mit stark gestiegenen Kosten für die IT-Sicherheit liegt in Unternehmen mit 50 bis unter 100 Mitarbeitern bei 36 Prozent, in Unternehmen mit 1.000 und mehr Mitarbeitern dagegen bei 47 Prozent (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 7251 (September 2016)

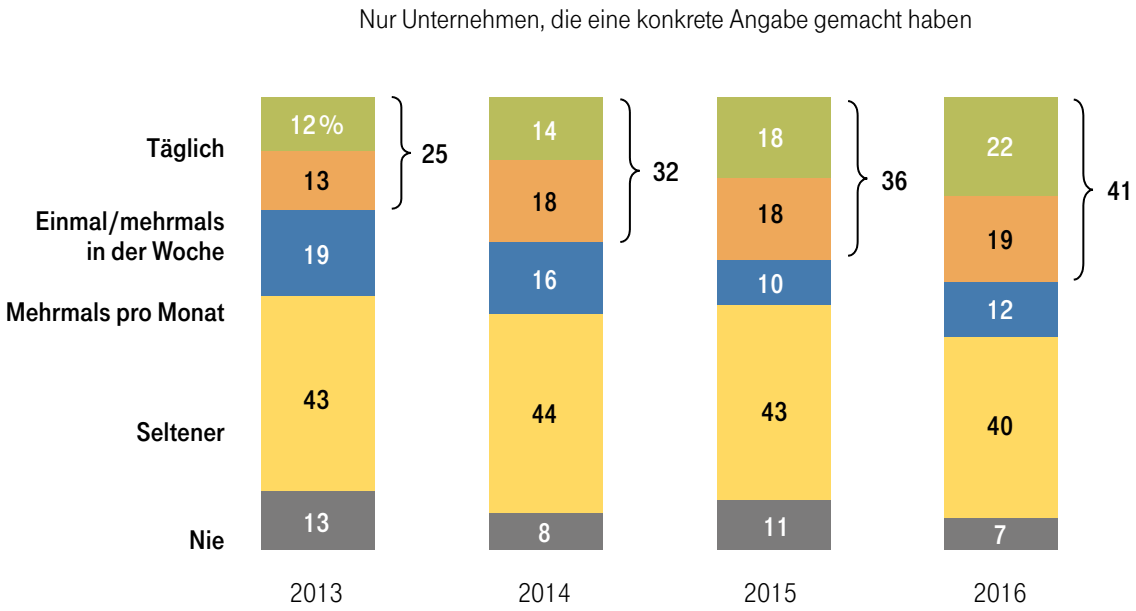
Schaubild 13

Der hohe Stellenwert der IT-Sicherheit in deutschen Unternehmen hat einen guten Grund: 93 Prozent der mittleren und großen Unternehmen waren bereits IT-Angriffen ausgesetzt, durch die das Unternehmen ausspioniert oder geschädigt werden sollte. 22 Prozent haben täglich, weitere 19 Prozent ein- oder mehrmals pro Woche mit externen Angriffe zu kämpfen, 12 Prozent mehrmals im Monat. Die Häufigkeit der (wahrgenommenen) Angriffe hängt dabei von der Größe des Unternehmens ab. So registrieren „nur“ 27 Prozent der Unternehmen mit 50 bis unter 100 Mitarbeitern mindestens einmal in der Woche IT-Angriffe, von den Unternehmen mit 1.000 und mehr Mitarbeitern sind es dagegen 56 Prozent. Umgekehrt geben 63 Prozent der Unternehmen mit 50 bis unter 100 Mitarbeitern zu Protokoll, höchstens einmal im Monat IT-Angriffen ausgesetzt zu sein; von den Unternehmen mit 1.000 und mehr Mitarbeitern ist es nur knapp ein Drittel (Schaubild 13).[1]

[1] 11 Prozent der Führungskräfte machten zur Häufigkeit der IT-Angriffe auf ihr Unternehmen keine konkrete Angabe, wobei es nur geringe Strukturunterschiede z. B. hinsichtlich der Mitarbeiterzahl oder des Umsatzes zwischen denjenigen Befragten gibt, die konkrete Angaben gemacht haben, und denjenigen ohne konkrete Angaben. 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 (vgl. tabellarischer Basisbericht).

HÄUFIGKEIT VON IT-ANGRIFFEN ERNEUT GESTIEGEN

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



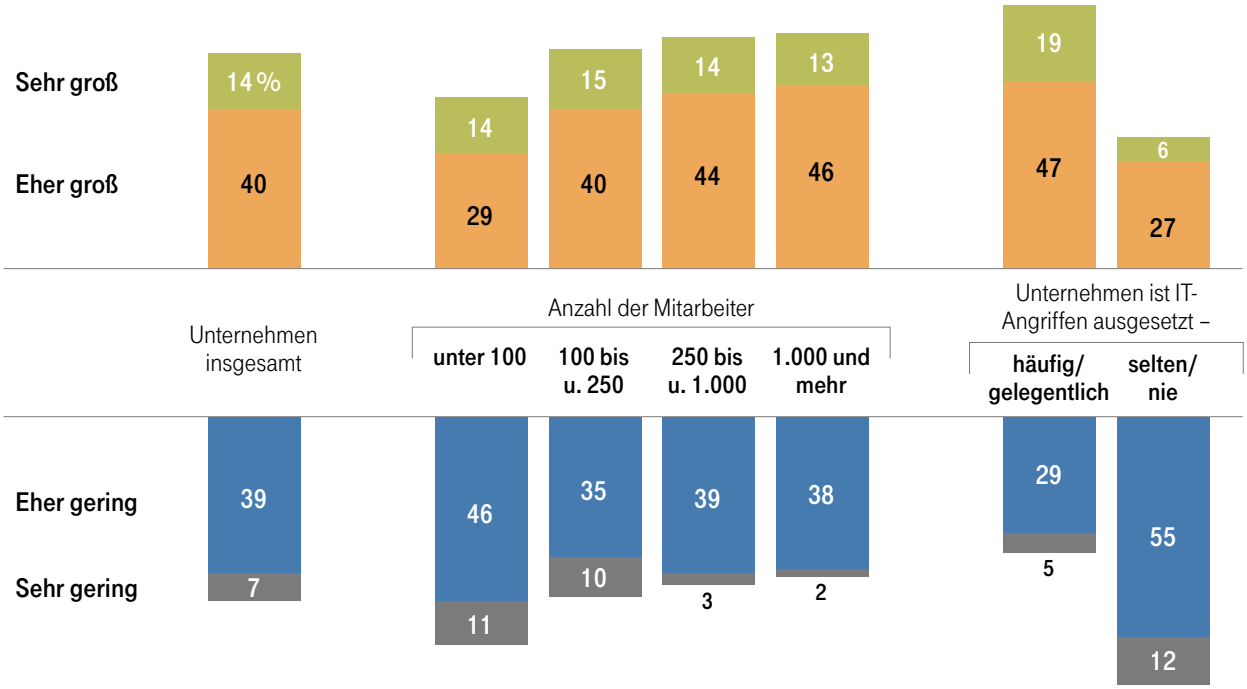
Basis: Bundesrepublik Deutschland; Führungskräfte in mittleren und großen Unternehmen, die eine konkrete Angabe zur Häufigkeit von IT-Angriffen gemacht haben
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7251 (September 2016)

Schaubild 14

Die Häufigkeit von IT-Angriffen auf deutsche Unternehmen ist in den vergangenen Jahren kontinuierlich gestiegen. Berichtete 2013 nur ein Viertel der mittleren und großen Unternehmen von mindestens wöchentlichen IT-Angriffen, sind es derzeit 41 Prozent (Schaubild 14).

EINE MEHRHEIT 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 7251 (September 2016)

Schaubild 15

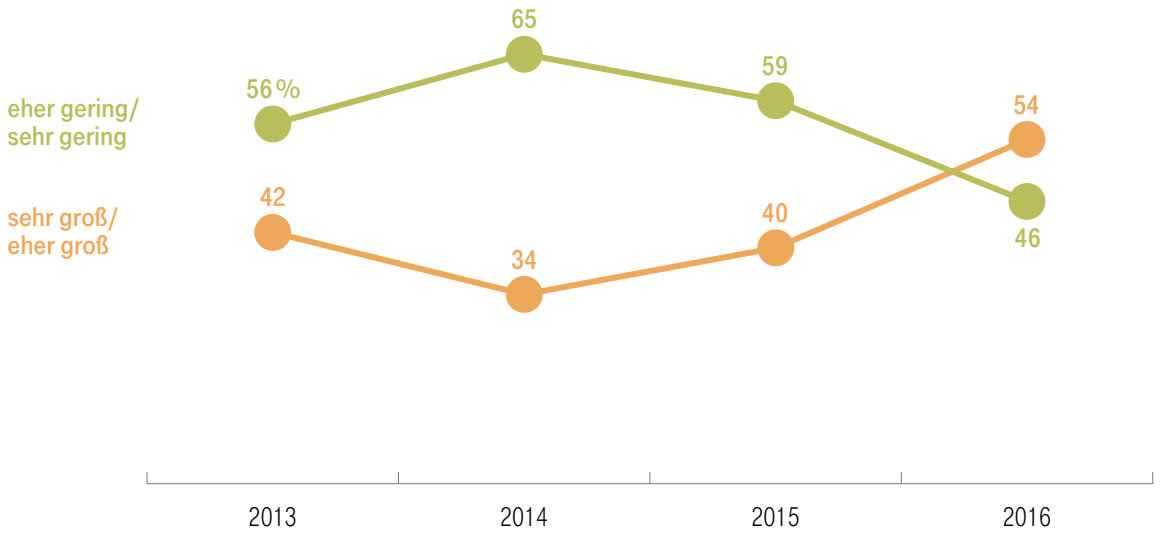
Zugleich stuft eine Mehrheit der mittleren und großen Unternehmen das Risiko, durch einen Hackerangriff gravierend geschädigt zu werden, als eher groß oder sogar sehr groß ein, darunter 14 Prozent, die ein sehr großes Risiko für gravierende Schäden sehen. Die Wahrnehmung des Risikos hängt dabei mit der Unternehmensgröße zusammen: Während in mittleren Unternehmen mit unter 100 Mitarbeitern eine Mehrheit der Führungskräfte hier nur ein eher geringes oder sehr geringes Risiko sieht, halten 59 Prozent der Führungskräfte aus großen Unternehmen mit 1.000 und mehr Mitarbeitern das Risiko, durch einen Hackerangriff gravierend geschädigt zu werden, für groß.

Gleichzeitig hängt die Risikoeinschätzung deutlich damit zusammen, wie häufig ein Unternehmen IT-Angriffe registriert. Von den Unternehmen, die über häufige oder gelegentliche IT-Angriffe berichten,[2] stufen rund zwei Drittel das Risiko gravierender Schäden durch solche Angriffe als groß bzw. sehr groß ein. Von den Unternehmen, die selten oder nie Ziel externer Angriffe sind, geht mit 33 Prozent ein nur halb so großer Anteil von einem (eher) großen Risiko aus, durch einen Hackerangriff gravierend geschädigt zu werden (Schaubild 15).

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

SUBJEKTIVE EINSCHÄTZUNG DES SCHADENSRISIKOS DURCH HACKERANGRIFFE IM ZEITVERLAUF

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



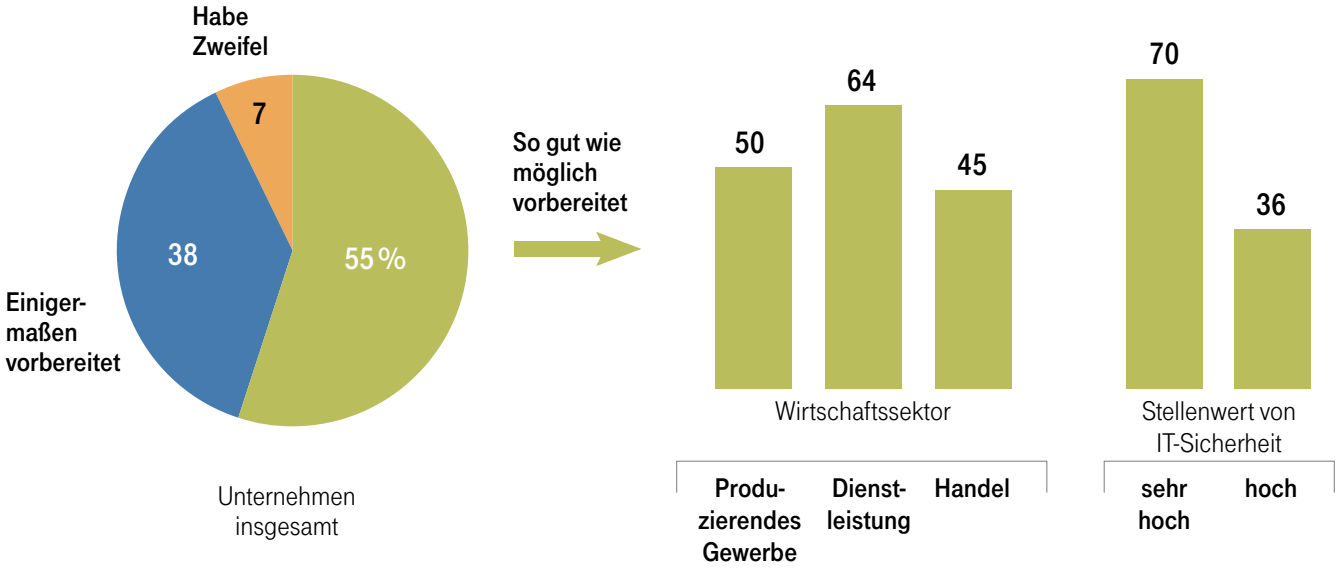
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7251 (September 2016)

Schaubild 16

Entsprechend dem kontinuierlich gestiegenen Anteil an Unternehmen, die von häufigen IT-Angriffen berichten, ist in den vergangenen beiden Jahren auch der Anteil der Führungskräfte deutlich angestiegen, der das Risiko für gravierende Schäden für das Unternehmen durch Hackerangriffe als eher groß oder sehr groß einschätzt. Dieser Anteil lag 2014 bei rund einem Drittel, aktuell bei 54 Prozent der Führungskräfte. Umgekehrt sind erstmals in den letzten Jahren die Führungskräfte, die ein (eher) geringes Schadenspotenzial sehen, in der Minderheit (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 7251 (September 2016)

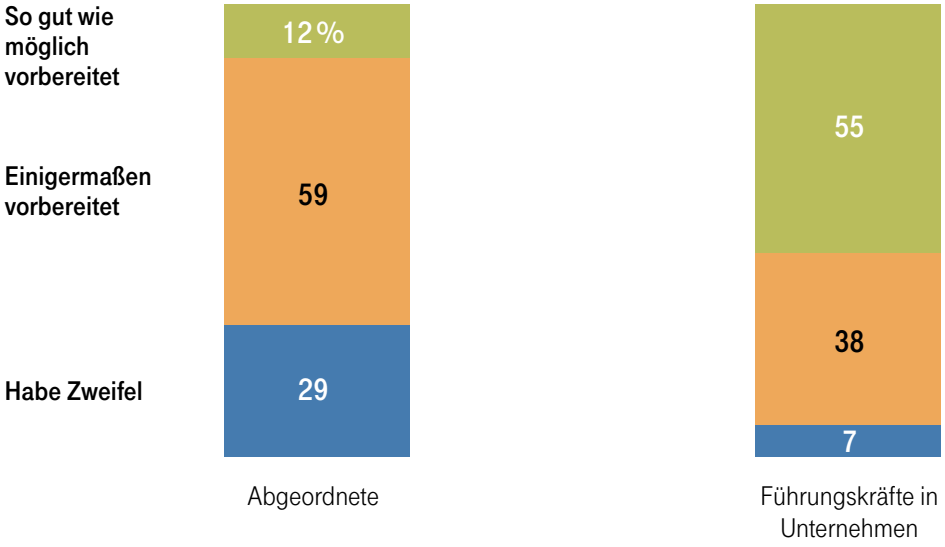
Schaubild 17

Dennoch sieht eine Mehrheit der Führungskräfte ihr eigenes Unternehmen so gut wie möglich auf Gefahren für die IT-Sicherheit vorbereitet, weitere 38 Prozent sehen ihr Unternehmen zumindest einigermaßen gerüstet. Lediglich 7 Prozent äußern dezidierte Zweifel daran. Unternehmen, die der IT-Sicherheit einen sehr hohen Stellenwert einräumen, sind nach Einschätzung ihrer Führungskräfte zu 70 Prozent bestmöglich auf Gefahren für die IT-Sicherheit vorbereitet, Unternehmen, bei denen die IT-Sicherheit „nur“ einen hohen – also keinen sehr hohen – Stellenwert genießt, dagegen nur zu 36 Prozent.

Wie gut Unternehmen gegen mögliche Gefahren für die IT-Sicherheit gewappnet sind, unterscheidet sich bemerkenswerterweise in den verschiedenen Wirtschaftssektoren. Während sich rund zwei Drittel der mittleren und großen Dienstleistungsunternehmen so gut wie möglich vorbereitet sehen, sind es im produzierenden Gewerbe 50 Prozent, im Handel 45 Prozent (Schaubild 17).

SIND DIE UNTERNEHMEN IN DEUTSCHLAND AUF IT-ANGRIFFE VORBEREITET? POLITIKER SIND DEUTLICH SKEPTISCHER ALS DIE FÜHRUNGSKRÄFTE IN DER WIRTSCHAFT.

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?“



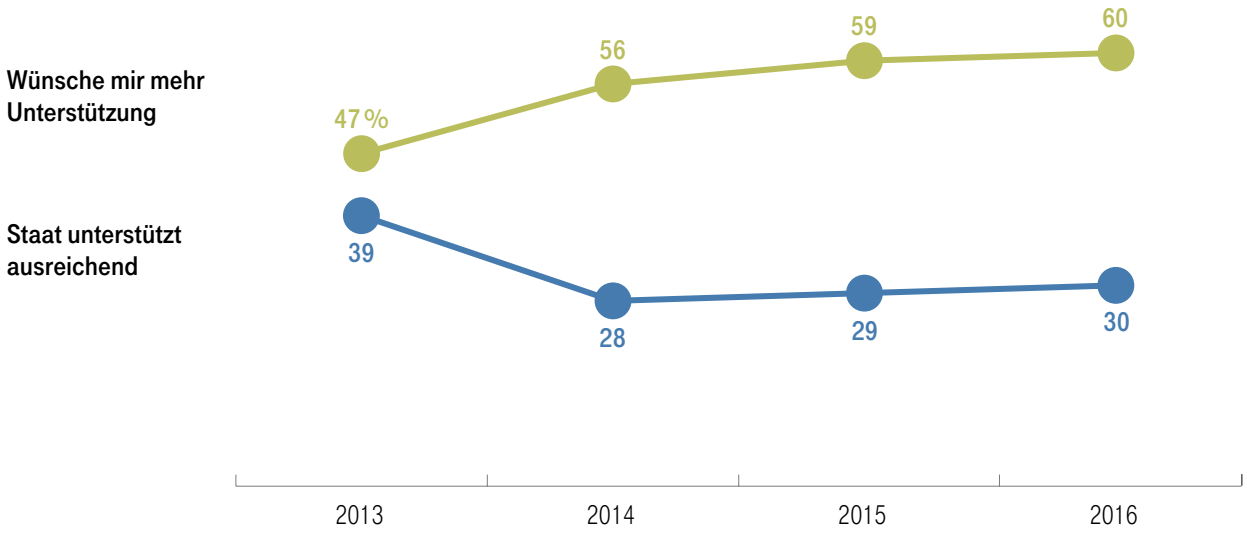
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 18

Während die Führungskräfte mehrheitlich von einer ausreichenden Vorbereitung des eigenen Unternehmens auf IT-Angriffe überzeugt sind, äußern sich Politiker eher skeptisch, sehen Unternehmen in Deutschland nur zu einem kleinen Teil so gut wie möglich auf z. B. Hackerangriffe vorbereitet. Nur 12 Prozent der Abgeordneten sind der Meinung, dass die Unternehmen in Deutschland bestmöglich gegen die Gefahren für ihre IT-Systeme gewappnet sind; 59 Prozent sehen die Unternehmen zumindest einigermaßen vorbereitet (Schaubild 18).

VERBREITETER 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

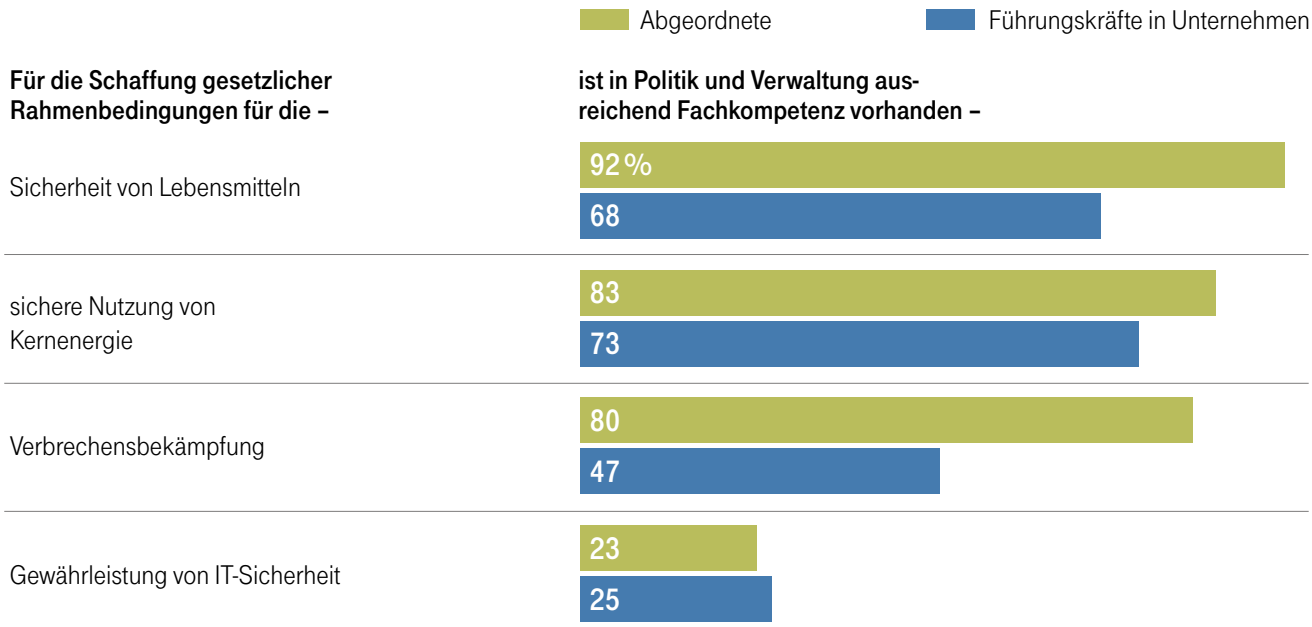
Quelle: Allensbacher Archiv, IfD-Umfragen, zuletzt 7251 (September 2016)

Schaubild 19

Für eine (noch) bessere Vorbereitung auf IT-Angriffe wünscht sich eine Mehrheit von 60 Prozent der Führungskräfte in mittleren und großen Unternehmen mehr Unterstützung vom Staat, nur 30 Prozent sehen sich bei dieser Aufgabe vom Staat ausreichend unterstützt. Der Anteil der Führungskräfte in der Wirtschaft, die nach mehr staatlicher Unterstützung rufen, liegt zwar deutlich höher als 2013, war in den letzten beiden Jahren aber annähernd stabil (Schaubild 19).

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 7251 (September 2016)

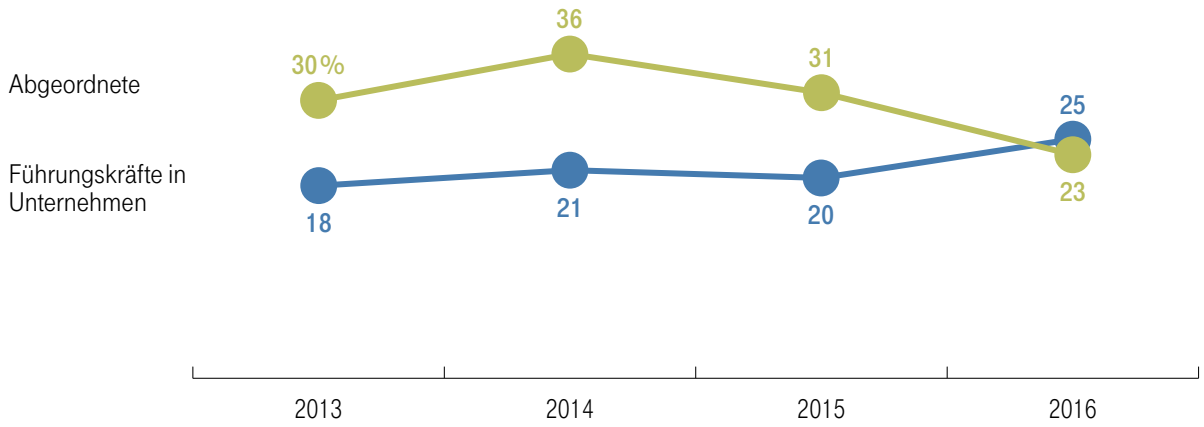
Schaubild 20

Aber auch wenn Führungskräfte aus der Wirtschaft verbreitet nach mehr Unterstützung durch den Staat bei der Sicherstellung von IT-Sicherheit rufen, sieht eine deutliche Mehrheit bei Politik und Verwaltung gleichzeitig keine ausreichende Fachkompetenz, um entsprechende gesetzliche Rahmenbedingungen zu schaffen. Und auch Politiker selbst zweifeln mehrheitlich daran, dass Legislative und Exekutive in der Lage sind, dieses Problem kompetent anzugehen.

Während in anderen Bereichen wie der Nutzung der Kernenergie oder der Sicherheit von Lebensmitteln eine deutliche Mehrheit sowohl der Wirtschaftsführer als auch der Abgeordneten Politik und Verwaltung eine hohe Fachkompetenz bescheinigt, hinkt die IT-Sicherheit deutlich hinterher. Von den Führungskräften in den Unternehmen sind gerade einmal 25 Prozent davon überzeugt, dass es auf staatlicher Seite ausreichende Fachkompetenz für die Schaffung gesetzlicher Rahmenbedingungen zur Gewährleistung von IT-Sicherheit gibt, von den Abgeordneten gehen sogar nur 23 Prozent davon aus, dass Politik und Verwaltung über genügend Know-how bezüglich dieses Themas verfügen (Schaubild 20).

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 7251 (September 2016)

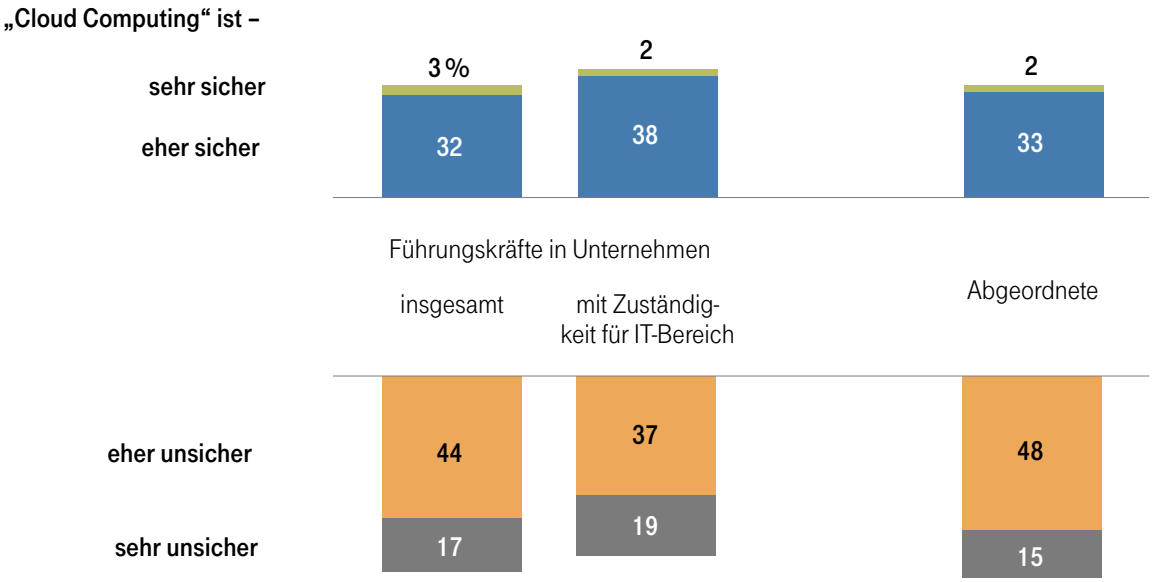
Schaubild 21

Während der Anteil derjenigen Unternehmensführer, die Politik und Verwaltung eine ausreichende Fachkompetenz beim Thema IT-Sicherheit bescheinigen, im vergangenen Jahr immerhin von 20 Prozent auf 25 Prozent gestiegen ist, hat sich die Wahrnehmung der Politiker in diesem Punkt in den letzten beiden Jahren deutlich negativ entwickelt. Während 2014 noch 36 Prozent der Abgeordneten Verwaltung und Politik in diesem Bereich für ausreichend kompetent hielten, liegt der Anteil mit aktuell 23 Prozent erstmals sogar unter dem entsprechenden Anteil bei den Wirtschaftsentscheidern (Schaubild 21).

NACH WIE VOR SPÜRBAR VERBREITETE SICHERHEITSBEDENKEN BEIM CLOUD COMPUTING, DENNOCH WERDEN HÄUFIG AUCH SENSIBLE DATEN IN DER CLOUD GESPEICHERT

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‘?“



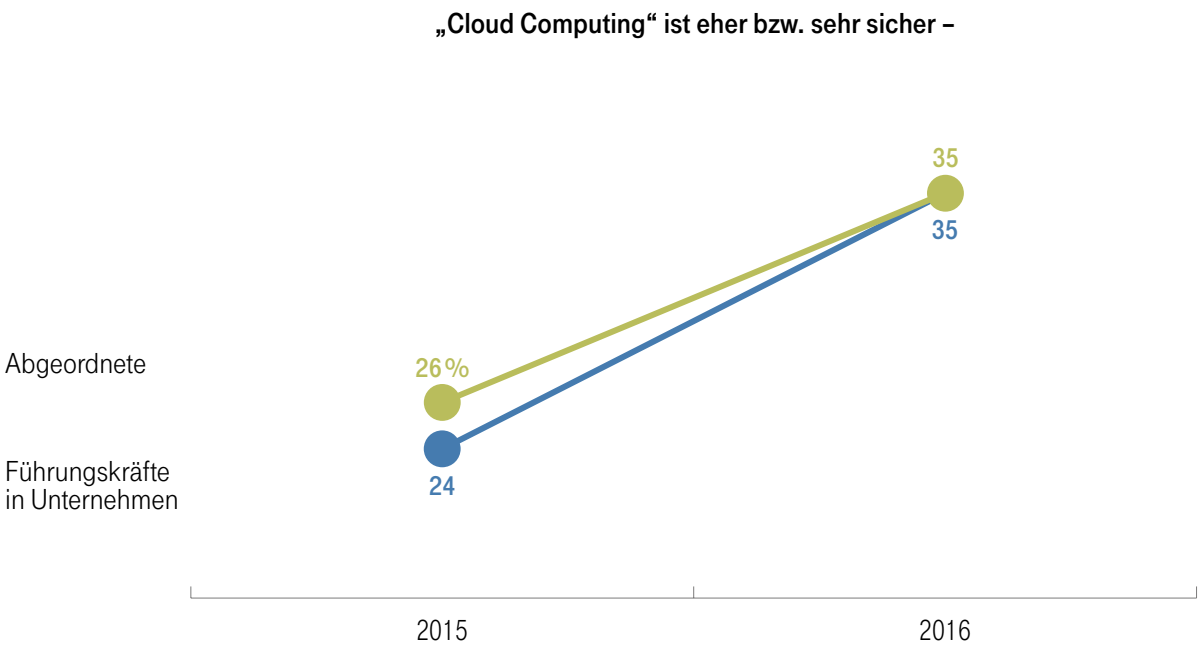
Auf 100 fehlende Prozent: Kommt darauf an, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 22

„Cloud Computing“, also die Möglichkeit, eigene Daten und Programme extern im Internet statt auf dem eigenen Computer oder Firmenserver zu speichern, stößt bei Entscheidern nach wie vor auf erhebliche Sicherheitsbedenken. Von den Führungskräften in mittleren und großen Unternehmen halten diese Art der Datenspeicherung nur 3 Prozent für sehr sicher, weitere 32 Prozent für eher sicher. Die Mehrheit hält Cloud Computing dagegen für eher unsicher (44 Prozent) oder sehr unsicher (17 Prozent). Führungskräfte, die in ihrem Unternehmen für den IT-Bereich verantwortlich sind, stehen Cloud Computing zwar tendenziell aufgeschlossener gegenüber. Aber auch sie sehen in Bezug auf dieses Thema die Datensicherheit mehrheitlich kritisch. Bei Abgeordneten stößt Cloud Computing auf ganz ähnliche Skepsis wie unter Entscheidern in der Wirtschaft. 35 Prozent der Politiker halten Cloud Computing für (eher) sicher, 63 Prozent dagegen für (eher) unsicher (Schaubild 22).

ABER DAS VERTRAUEN IN „CLOUD COMPUTING“ IST IM VERGANGENEN JAHR DEUTLICH GESTIEGEN



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 7231 (September 2015), 7251 (September 2016)

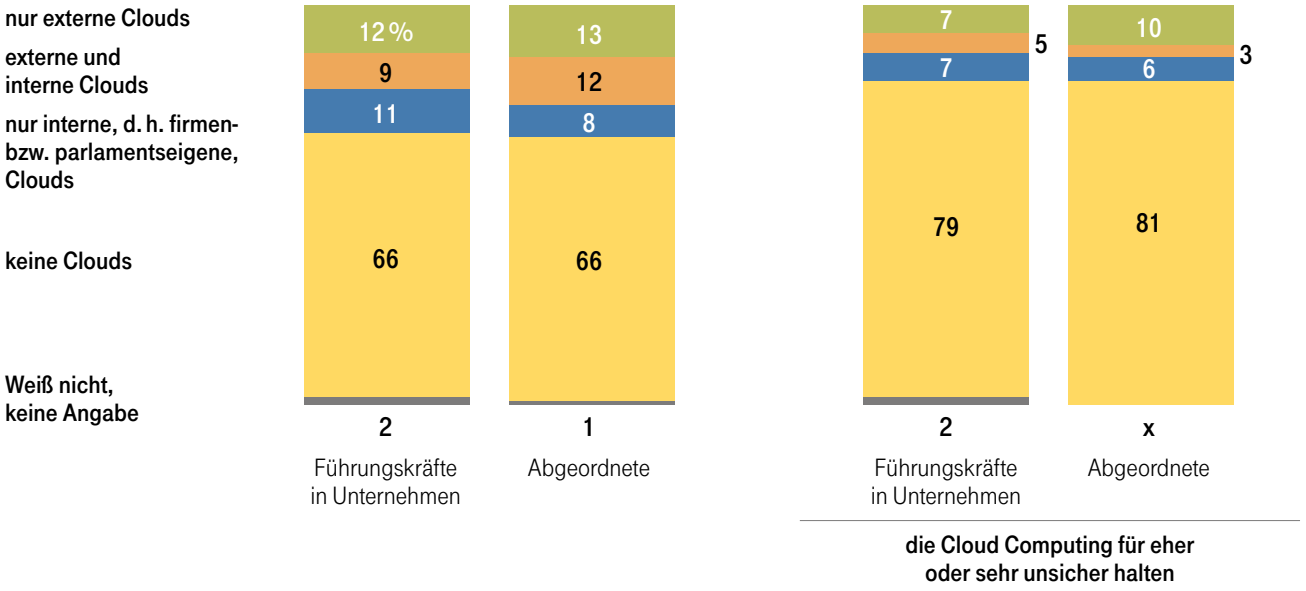
Schaubild 23

Dabei ist das Vertrauen der Entscheider in die Datensicherheit beim „Cloud Computing“ im letzten Jahr signifikant gestiegen: Während 2015 nur 26 Prozent der Abgeordneten und 24 Prozent der Wirtschaftsführer „Cloud Computing“ für sehr bzw. eher sicher hielten, sind es in beiden Gruppen aktuell 35 Prozent (Schaubild 23).

SICHERHEITSBEDENKEN HALTEN NICHT IN JEDEM FALL VON DER NUTZUNG VON CLOUD-DIENSTEN AB

Frage: „Nutzen Sie für Geschäftliches/Dienstliches Cloud-Dienste? Ich meine jetzt, egal ob firmen-/parlamentseigene Clouds oder Clouds externer Anbieter."

Es nutzen geschäftlich/dienstlich –



x = unter 0,5 Prozent

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 24

Insgesamt berichten jeweils rund ein Drittel der Abgeordneten und ein Drittel der Führungskräfte mittlerer und großer Unternehmen, Cloud-Dienste für geschäftliche bzw. dienstliche Zwecke zu nutzen. Darunter geben 12 Prozent der Wirtschaftsführer zu Protokoll, dass sie ausschließlich Clouds externer Anbieter nutzen, 11 Prozent, dass sie nur interne, d. h. firmeneigene, Clouds nutzen, und 9 Prozent, dass sie auf beides, d. h. sowohl auf externe als auch auf interne Cloud-Angebote, zurückgreifen.

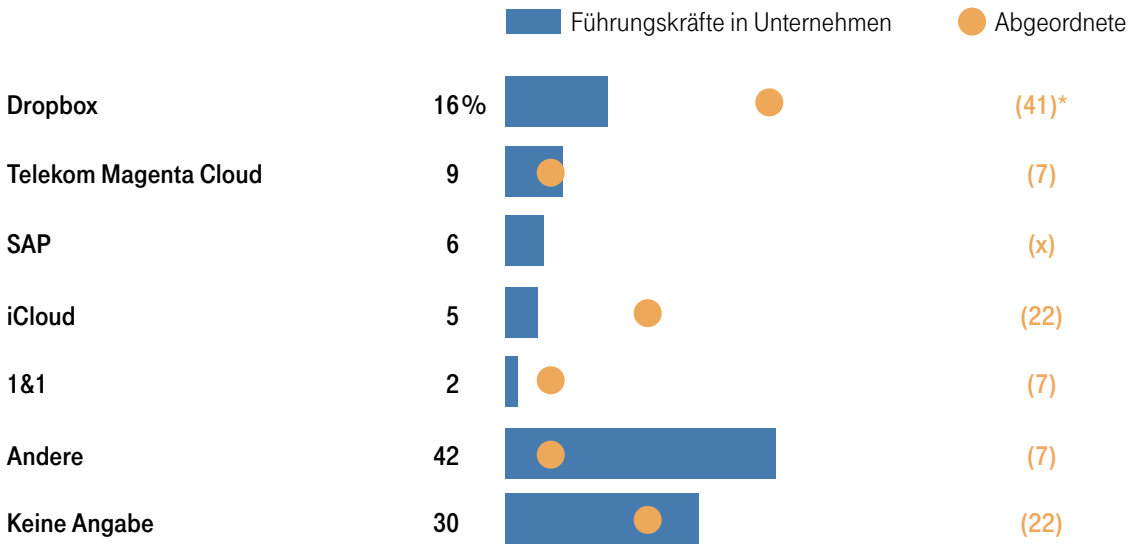
Die Abgeordneten berichten von einer ganz ähnlichen Nutzung von Cloud-Angeboten: 13 Prozent nutzen ausschließlich externe Angebote, 8 Prozent nur parlamentseigene Cloud-Dienste und 12 Prozent beide Arten von Cloud-Diensten.

Entscheider, die die Datensicherheit beim Cloud Computing kritisch sehen, nutzen Cloud-Dienste zwar in kleinerem Umfang als der Durchschnitt der Entscheider. Aber immerhin knapp jeder fünfte Entscheider aus Wirtschaft und Politik, der Cloud Computing für eher oder sehr unsicher hält, räumt ein, solche Dienste in Anspruch zu nehmen. Sicherheitsbedenken halten offenbar in vielen Fällen nicht von der Nutzung von Cloud-Diensten ab (Schaubild 24).

POLITIKER NUTZEN VOR ALLEM DROPBOX UND ICLOUD, WIRTSCHAFTSFÜHRER EIN BREITES SPEKTRUM VON ANBIETERN

Als externen Anbieter nutzen –
(Mehrfachangaben möglich)

Nutzer externer Cloud-Dienste



*( ) Wegen geringer Fallzahl (n = 27) nur als Tendenzbefund zu interpretieren.
x = unter 0,5 Prozent

Basis: Bundesrepublik Deutschland: Abgeordnete und Führungskräfte in Unternehmen, die externe Cloud-Dienste nutzen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 25

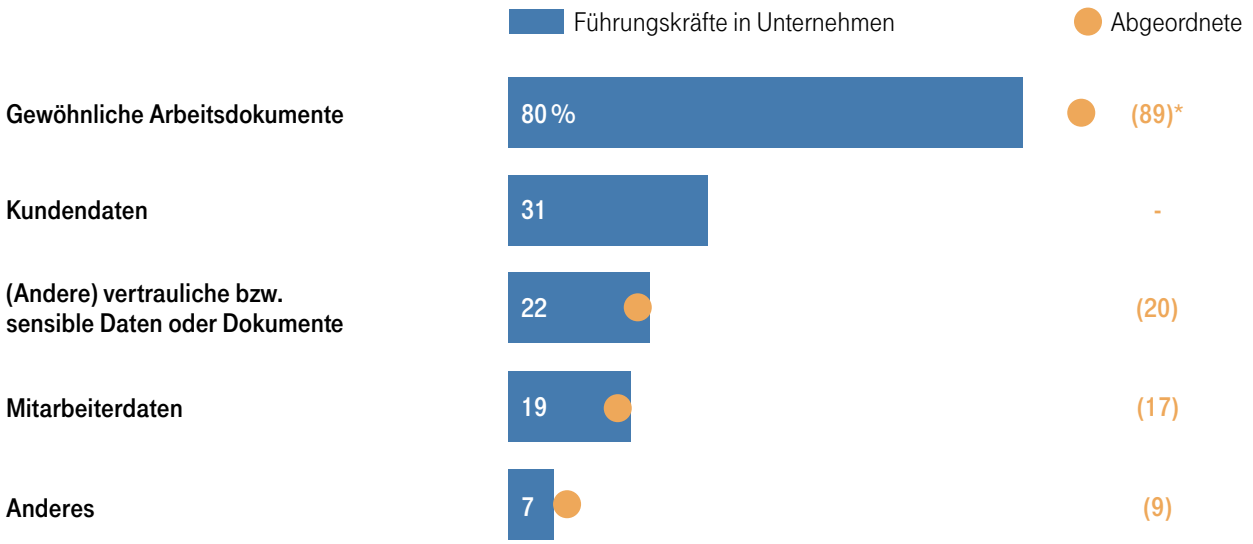
Dabei nutzen Abgeordnete als externen Cloud-Anbieter mit Abstand am häufigsten Dropbox.[3] Führungskräfte in Unternehmen geben dagegen ein sehr breites Spektrum genutzter Angebote zu Protokoll, ohne dass hier ein Anbieter herausragen würde (Schaubild 25).

[3] Wegen der geringen Fallzahl in dieser Teilgruppe (n = 27) kann dieses Ergebnis nur als Tendenzbefund interpretiert werden.

DER CLOUD WERDEN HÄUFIG AUCH VERTRAULICHE ODER SENSIBLE DATEN ANVERTRAUT

In der Cloud speichern –
(Mehrfachangaben möglich)

Nutzer von (internen und/oder externen) Clouds



*( ) Wegen geringer Fallzahl (n = 35) nur als Tendenzbefund zu interpretieren.

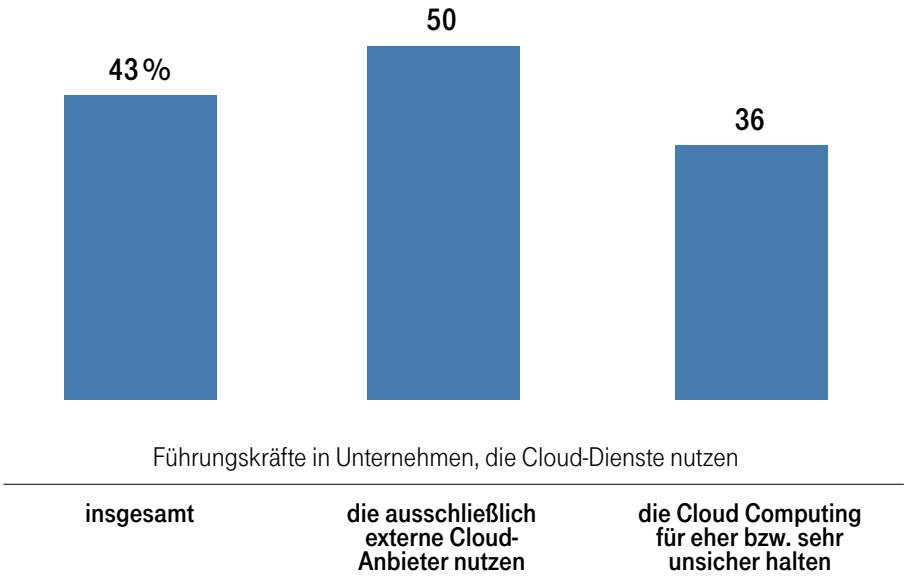
Basis: Bundesrepublik Deutschland: Abgeordnete und Führungskräfte in Unternehmen, die Cloud-Dienste nutzen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 26

Mit Abstand am häufigsten werden in (internen oder externen) Clouds gewöhnliche Arbeitsdokumente gespeichert. Bemerkenswert häufig werden aber auch vertrauliche Daten wie Kundendaten, Mitarbeiterdaten oder andere nicht öffentliche bzw. sensible Daten oder Dokumente der Cloud anvertraut (Schaubild 26).

SENSIBLE DATEN IN DER CLOUD – TROTZ SICHERHEITSBEDENKEN

In der Cloud speichern Kundendaten, Mitarbeiterdaten und/oder andere vertrauliche bzw. sensible Daten oder Dokumente –



Basis: Bundesrepublik Deutschland: Führungskräfte in Unternehmen, die Cloud-Dienste nutzen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

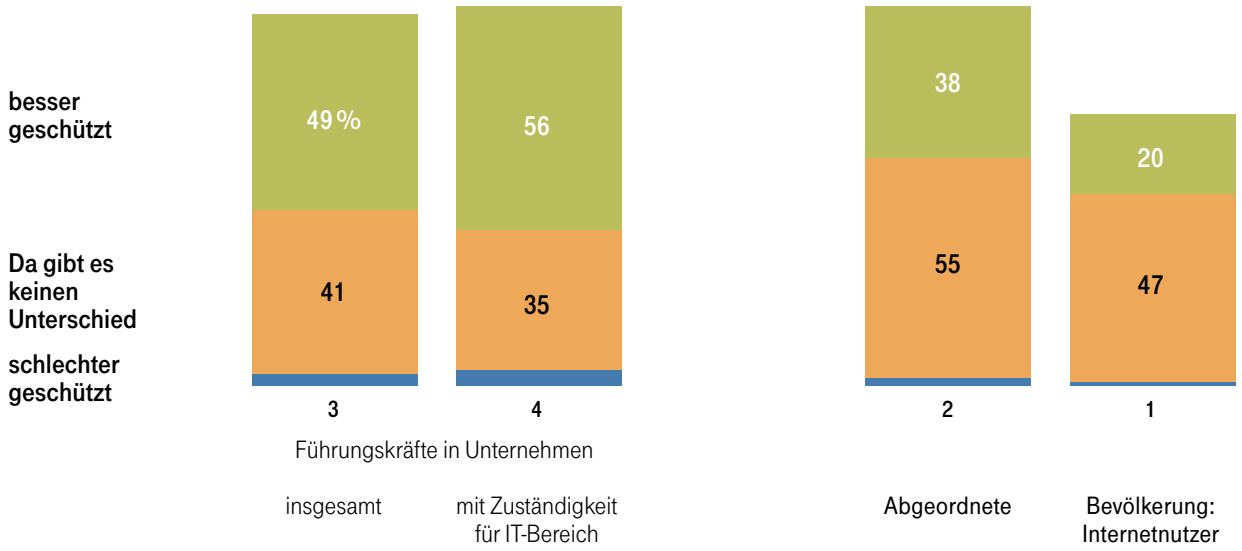
Schaubild 27

So speichert die Hälfte der Unternehmen, die ausschließlich externe Cloud-Angebote nutzen, solche vertraulichen Daten außerhalb des eigenen Kontrollbereichs online ab. Und selbst von denjenigen Führungskräften, die ausdrücklich Zweifel an der Datensicherheit beim Cloud Computing äußern, legt ein gutes Drittel dennoch Kundendaten, Mitarbeiterdaten und/oder andere vertrauliche oder sensible Dokumente oder Daten in die Hände der Cloud (Schaubild 27).

VOR ALLEM WIRTSCHAFTSFÜHRER TRAUEN DEUTSCHEN CLOUD-ANBIETERN BEIM DATENSCHUTZ EHER ALS AMERIKANISCHEN

Frage: „Was denken Sie: Sind Dateien bei einem deutschen Cloud-Anbieter besser vor Datenmissbrauch geschützt als bei einem amerikanischen Cloud-Anbieter oder schlechter geschützt oder gibt es da keinen Unterschied?“

Daten sind bei einem deutschen Cloud-Anbieter im Vergleich zu einem amerikanischen Anbieter –



Auf 100 fehlende Prozent: Schwer zu sagen, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen bzw. Bevölkerung ab 16 Jahren
Quelle: Allensbacher Archiv, IfD-Umfragen 11059 (August 2016), 7251 (September 2016)

Schaubild 28

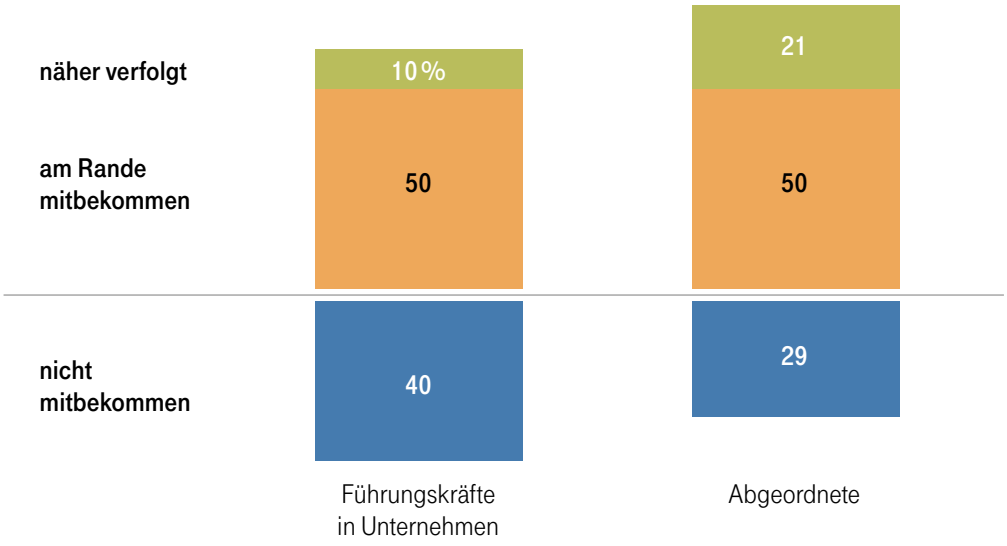
Auch wenn das Vertrauen in die Datensicherheit von Cloud-Lösungen insgesamt eher gering ist, machen Entscheider doch einen Unterschied im Hinblick auf den Sitz des Anbieters. So zeigen sich rund die Hälfte der Führungskräfte aus der Wirtschaft und 38 Prozent der Abgeordneten davon überzeugt, dass Daten bei einem deutschen Cloud-Anbieter besser vor Missbrauch geschützt sind als bei einem amerikanischen. Führungskräfte aus mittleren und großen Unternehmen, die für den IT-Bereich zuständig sind, vertreten diese Auffassung sogar mehrheitlich. Umgekehrt urteilt dagegen kaum ein Befragter, dass der Schutz bei einem amerikanischen Anbieter besser sei als bei einem deutschen.

In der Urteilstendenz entspricht dies auch der Wahrnehmung der Bevölkerung, auch wenn hier vergleichsweise größere Teile kein Urteil abgeben bzw. eine deutliche relative Mehrheit keinen Unterschied zwischen deutschen und amerikanischen Anbietern sieht (Schaubild 28).

VIELE ENTSCHEIDER WISSEN VOM „PRIVACY SHIELD“-ABKOMMEN DER EU MIT DEN USA NICHTS

Frage: „Im Jahr 2015 wurde das Datenschutzabkommen zwischen der EU und den USA, das sogenannte ‚Safe Harbor‘-Abkommen, vom Europäischen Gerichtshof für ungültig erklärt. Seit Mitte dieses Jahres ist dafür der ‚EU-US Privacy Shield‘ in Kraft. Haben Sie das näher verfolgt oder nur am Rande mitbekommen oder gar nicht mitbekommen?“

Die Vorgänge um das „Privacy Shield“-Abkommen haben –



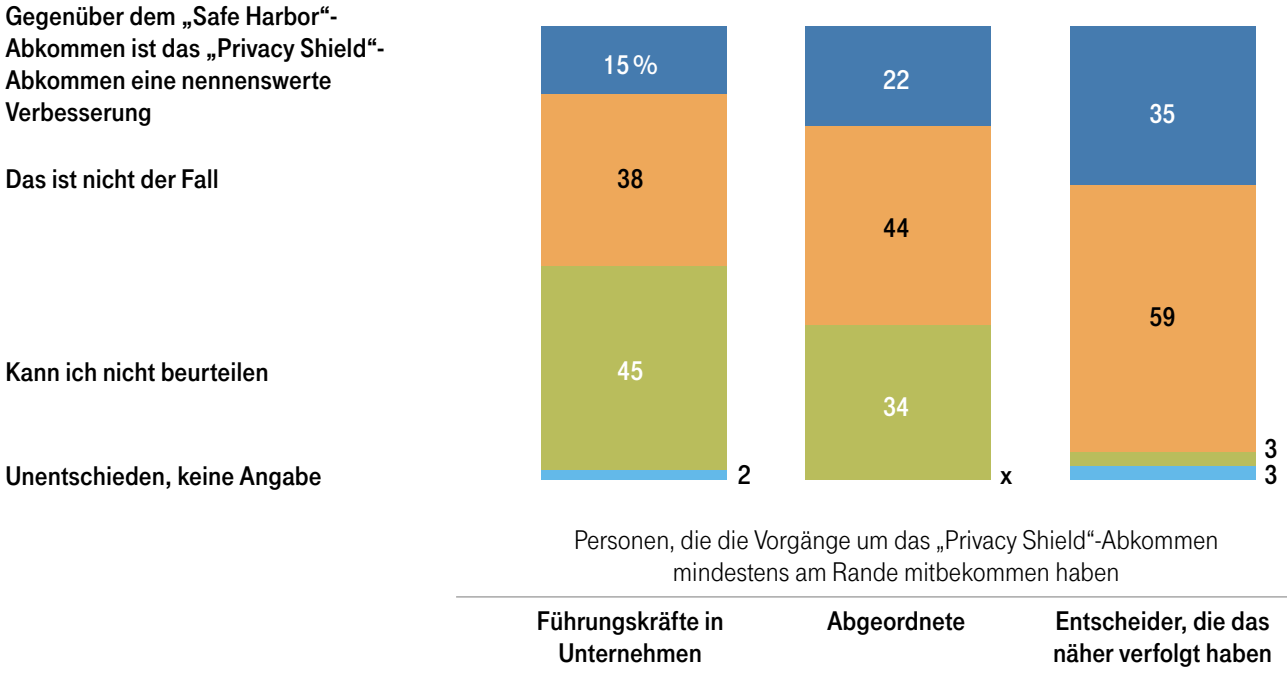
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 29

Von dem im Juli 2016 in Kraft getretenen „Privacy Shield“-Abkommen zwischen der EU und den USA, das den Datenschutz speziell von personenbezogenen Daten regelt, die von einem EU-Land in die USA übertragen werden, haben viele Entscheider keine Kenntnis. Nur 10 Prozent der Top-Entscheider in mittleren und großen Unternehmen und 21 Prozent der Abgeordneten haben die Vorgänge um dieses Abkommen näher verfolgt, jeweils weitere 50 Prozent haben das „am Rande mitbekommen“ (Schaubild 29).

NUR EINE KLEINE MINDERHEIT SIEHT IM „PRIVACY SHIELD“-ABKOMMEN EINE VERBESSERUNG IM VERGLEICH ZUM „SAFE HARBOR“-ABKOMMEN

Frage: „Halten Sie ‚Privacy Shield‘ für eine nennenswerte Verbesserung gegenüber dem ‚Safe Harbor‘-Abkommen oder ist das nicht der Fall?“



x = unter 0,5 Prozent

Basis: Bundesrepublik Deutschland; Abgeordnete und Führungskräfte in Unternehmen, die die Vorgänge um das „Privacy Shield“-Abkommen mindestens am Rande mitbekommen haben

Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 30

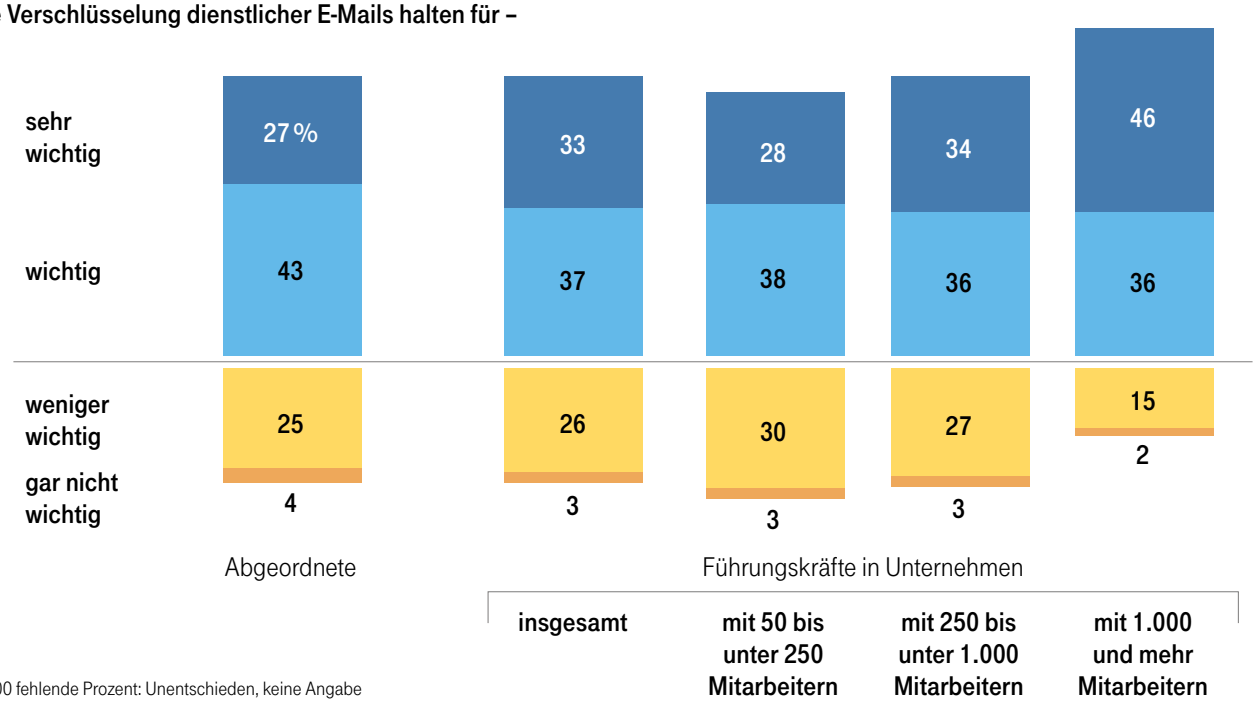
Von denjenigen Entscheidern, die die Vorgänge um das „Privacy Shield“-Abkommen zumindest am Rande mitbekommen haben, hat nur eine Minderheit den Eindruck, dass dieses Abkommen im Vergleich zum Vorgängervertrag, dem „Safe Harbor“-Abkommen, eine nennenswerte Verbesserung mit sich bringt. Viele trauen sich in dieser Frage allerdings auch kein Urteil zu. Von den Entscheidern, die die Vorgänge um das „Privacy Shield“-Abkommen näher verfolgt haben, sehen nur 35 Prozent eine Verbesserung gegenüber dem – vom Europäischen Gerichtshof gekippten – „Safe Harbor“-Abkommen, 59 Prozent widersprechen dem ausdrücklich (Schaubild 30).

DIENSTLICHE E-MAILS: HÄUFIG UNVERSCHLÜSSELT, ZUM TEIL AUCH VON PRIVATEN ACCOUNTS

DER VERSCHLÜSSELUNG DIENSTLICHER E-MAILS WIRD EINE HOHE BEDEUTUNG BEIGEMESSEN

Frage: „Für wie wichtig halten Sie es grundsätzlich, dass Ihre dienstlichen E-Mails durch eine Verschlüsselung geschützt werden? Halten Sie das für ...“

Eine Verschlüsselung dienstlicher E-Mails halten für –



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 31

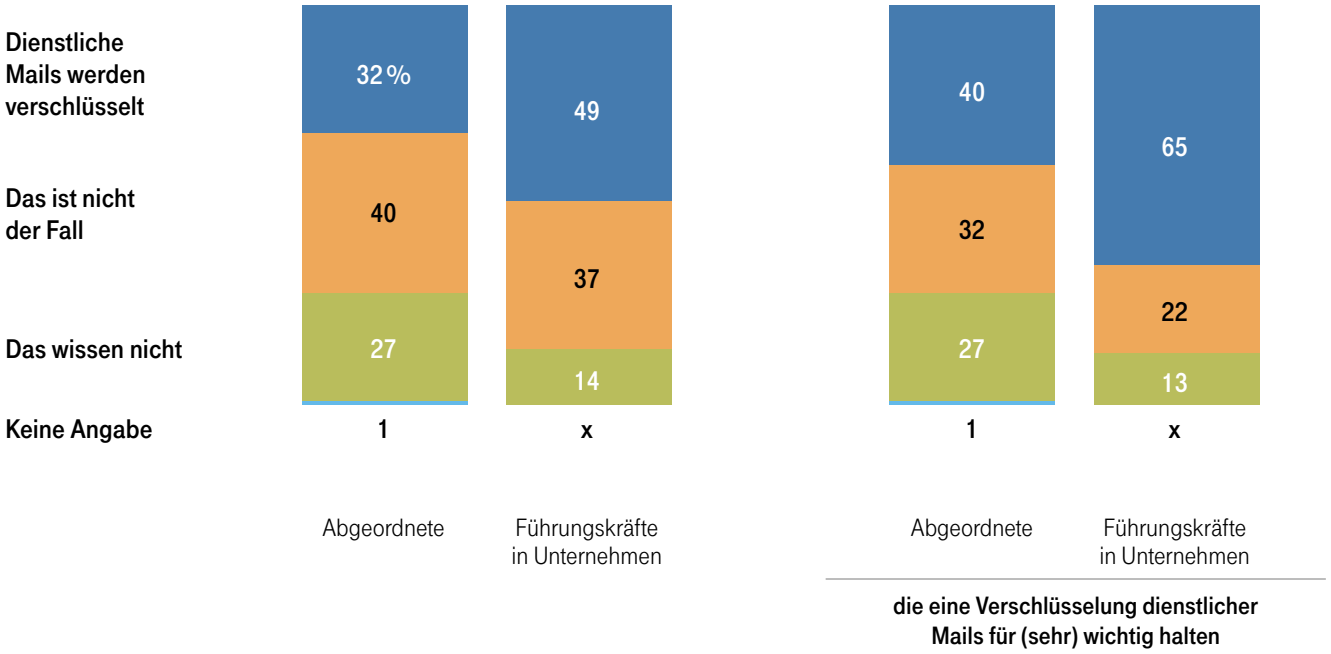
IT-Sicherheit hat für große und mittlere Unternehmen in Deutschland eine hohe Bedeutung.[4] Entsprechend wird auch die Verschlüsselung dienstlicher E-Mails häufig als wichtig erachtet: Rund ein Drittel der Führungskräfte hält das sogar für sehr wichtig, weitere 37 Prozent erachten das für wichtig. Ein überdurchschnittlicher Anteil der Führungskräfte großer Unternehmen mit 1.000 und mehr Mitarbeitern hält eine Verschlüsselung dienstlicher E-Mails für sehr wichtig (46 Prozent) oder wichtig (36 Prozent, d. h. zusammen 82 Prozent).

Die Bedeutung, die Abgeordnete der Verschlüsselung von E-Mails beimessen, liegt auf ähnlichem Niveau: Insgesamt 70 Prozent halten das für sehr wichtig oder wichtig (Schaubild 31).

[4] Vgl. Schaubild 11, Seite 16.

VIELE ENTSCHEIDUNGSTRÄGER VERSENDEN DIENSTLICHE E-MAILS UNVERSCHLÜSSELT

Frage: „Wissen Sie das zufällig: Werden Ihre dienstlichen E-Mails verschlüsselt oder ist das nicht der Fall?“



x = unter 0,5 Prozent

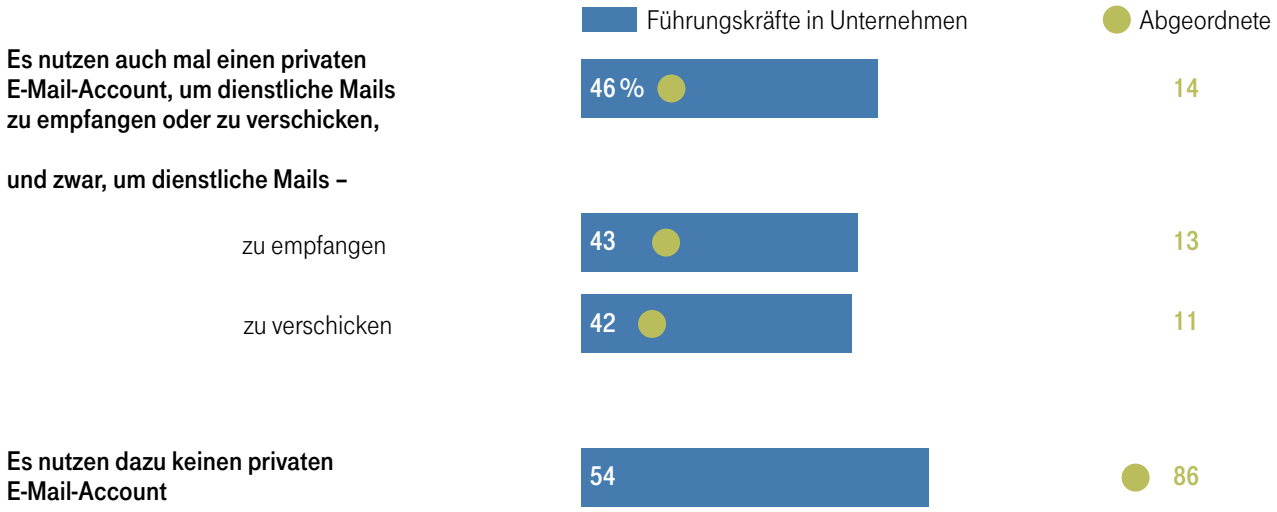
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 32

Dennoch versenden 40 Prozent der Abgeordneten und 37 Prozent der Führungskräfte in mittleren und großen Unternehmen ihre dienstlichen E-Mails unverschlüsselt, weitere 27 Prozent bzw. 14 Prozent wissen nicht, ob ihre Mails verschlüsselt werden. Selbst von denjenigen Entscheidern, die eine Verschlüsselung für wichtig oder sehr wichtig halten, wendet ein erheblicher Teil keine Verschlüsselungstechnik an: von den Abgeordneten rund ein Drittel und von den Wirtschaftsführern 22 Prozent (Schaubild 32).

POLITIKER NUTZEN VERBREITET PRIVATE ACCOUNTS, UM DIENSTLICHE E-MAILS ZU VERSCHICKEN



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 33

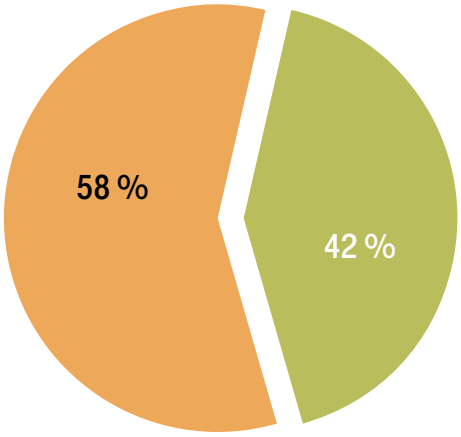
Dies ist im Zusammenhang mit dem E-Mail-Verkehr von Verantwortungsträgern aber nicht der einzige unter Sicherheitsaspekten bedenkliche Punkt. Fast die Hälfte der Abgeordneten nutzt auch mal einen privaten Account, um dienstliche E-Mails zu empfangen oder zu versenden. Hillary Clintons Umgang mit E-Mails ist offenbar kein Einzelfall. Unter Führungskräften in großen und mittleren Unternehmen ist diese Praxis weit weniger verbreitet. Aber auch hier räumt immerhin rund jeder Siebte ein, auch mal einen privaten Account für geschäftliche Mails zu nutzen (Schaubild 33).

DIENSTLICHE E-MAILS VOM PRIVATEN ACCOUNT: MEISTENS UNVERSCHLÜSSELT

Frage: „Schützen Sie diese E-Mails, die Sie über einen privaten Account versenden, durch eine Verschlüsselung, d. h., verschlüsseln Sie sie selbst bzw. benutzen Sie einen E-Mail-Anbieter, der die E-Mails verschlüsselt, oder schützen Sie Ihre Mails nicht durch eine Verschlüsselung?“

Abgeordnete und Führungskräfte in Unternehmen, die auch mal einen privaten Account nutzen, um dienstliche Mails zu versenden –

Es schützen ihre dienstlichen E-Mails **nicht** durch eine Verschlüsselung, wenn sie diese von einem privaten Account versenden



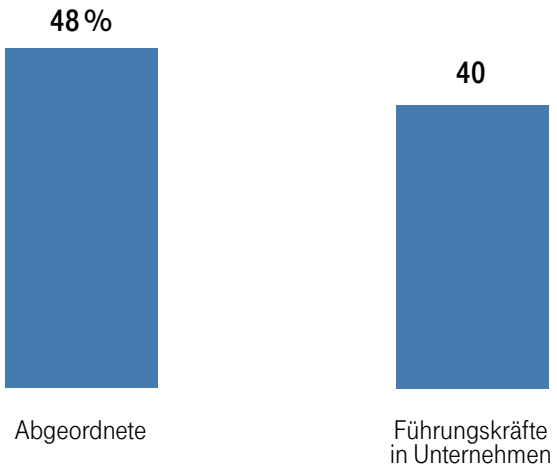
Basis: Bundesrepublik Deutschland: Abgeordnete und Führungskräfte in Unternehmen, die auch mal einen privaten Account nutzen, um dienstliche Mails zu verschicken
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 34

Und die von privaten Accounts versendeten Mails sind noch seltener durch eine Verschlüsselung geschützt als bei dienstlichen Accounts: 58 Prozent der Entscheider, die auch mal einen privaten Account nutzen, um dienstliche Mails zu versenden, wissen, dass diese Mails unverschlüsselt verschickt werden (Schaubild 34).

DIENSTLICHE E-MAILS: VERBREITET SICHERHEITSDEFIZITE

Es verschlüsseln ihre dienstlichen E-Mails generell nicht oder nutzen auch mal einen privaten Account, um dienstliche Mails unverschlüsselt zu senden –



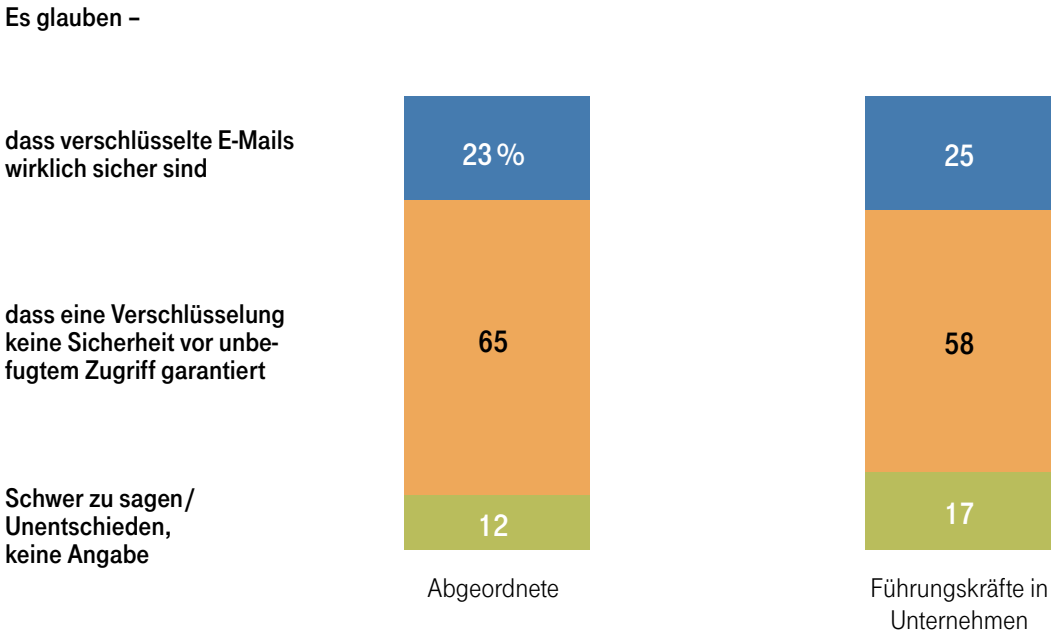
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 35

Insgesamt versenden rund die Hälfte der Abgeordneten und 40 Prozent der Führungskräfte in mittleren und großen Unternehmen dienstliche Mails (auch) unverschlüsselt, sei es, dass dienstliche Mails generell nicht verschlüsselt werden, sei es, dass dienstliche Mails auch mal über einen unverschlüsselten privaten Account versandt werden (Schaubild 35).

GERINGES VERTRAUEN IN DIE SICHERHEIT VON E-MAIL-VERSCHLÜSSELUNGEN

Frage: „Glauben Sie, dass verschlüsselte E-Mails auch wirklich sicher sind, also dass Unbefugte nicht darauf zugreifen können, oder garantiert eine Verschlüsselung keine Sicherheit vor unbefugtem Zugriff?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

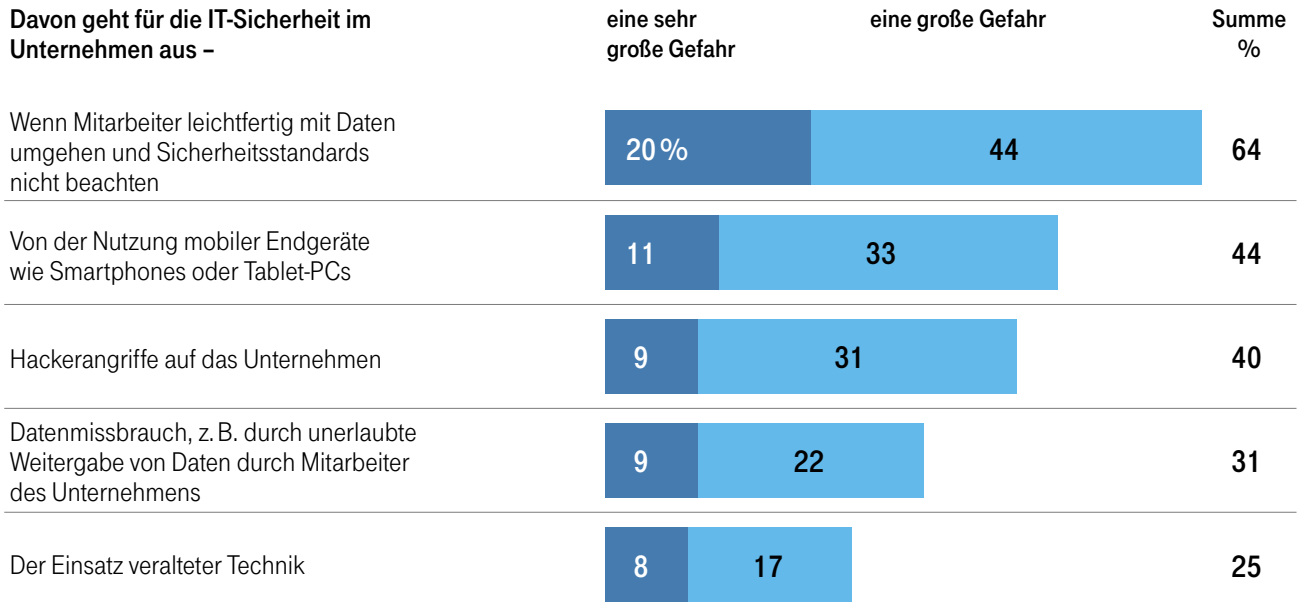
Schaubild 36

Allerdings ist das Vertrauen der Führungskräfte aus Politik und Wirtschaft in die Sicherheit von E-Mail-Verschlüsselungen auch eher gering. Nur jeweils rund ein Viertel der Abgeordneten und der Entscheider aus der Wirtschaft geht davon aus, dass verschlüsselte E-Mails wirklich sicher sind. In beiden Gruppen ist die Mehrheit ausdrücklich davon überzeugt, dass auch eine Verschlüsselung keine Sicherheit vor unbefugtem Zugriff garantiert (65 Prozent bzw. 58 Prozent, Schaubild 36).

SICHERHEITSLÜCKE SMARTPHONE

GEFAHRENQUELLEN FÜR DIE IT-SICHERHEIT IM EIGENEN UNTERNEHMEN

Frage: „Wovon geht Ihrer Meinung nach eine besondere Gefahr für die IT-Sicherheit in Ihrem Unternehmen aus? Wovon geht eine sehr große, eine große, eine weniger große oder kaum eine Gefahr aus?“



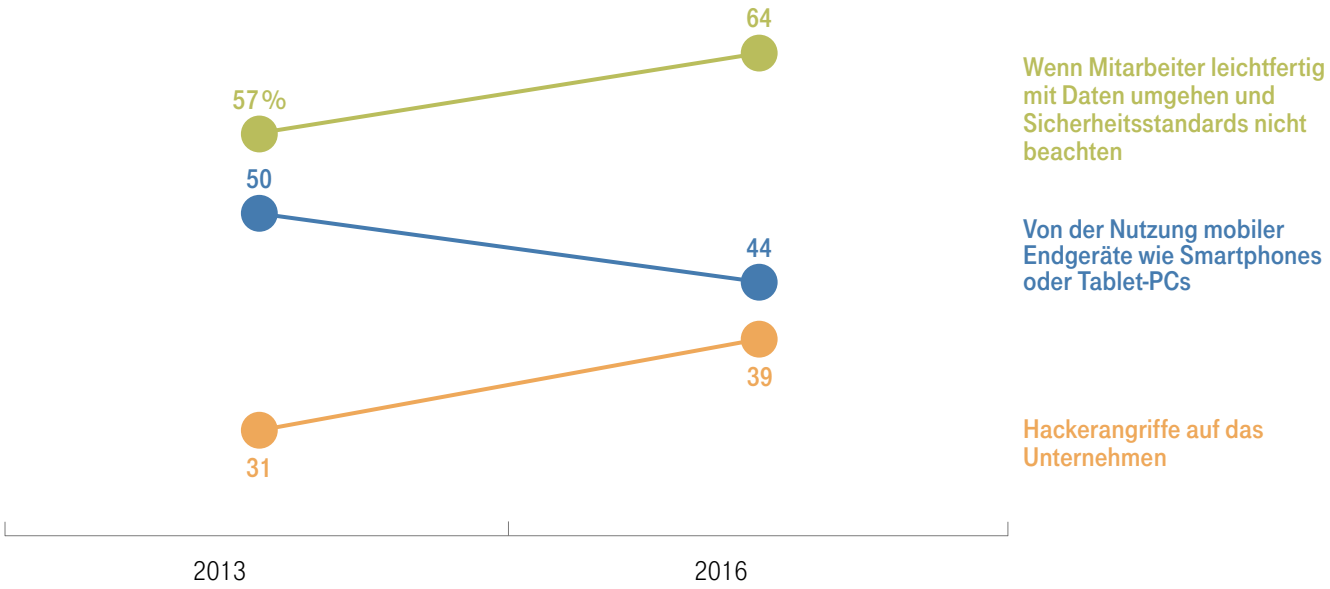
Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 37

Mit Abstand am häufigsten sehen Führungskräfte aus mittleren und großen Unternehmen Gefahren für die IT-Sicherheit in einem leichtfertigen Umgang von Mitarbeitern mit Daten bzw. der Missachtung von Sicherheitsstandards. Rund zwei Drittel der Führungskräfte sehen davon große oder sogar sehr große Gefahren für die IT-Sicherheit des eigenen Unternehmens ausgehen. Mit 44 Prozent am zweithäufigsten werden (sehr) große Gefahren durch die Nutzung mobiler Endgeräte wie Smartphones oder Tablet-PCs befürchtet, 40 Prozent sehen (sehr) große Gefahren durch Hackerangriffe auf das Unternehmen (Schaubild 37).

FÜHRUNGSKRÄFTE IN DER WIRTSCHAFT SEHEN DIE IT-SICHERHEIT IHRER UNTERNEHMEN HEUTE STÄRKER DURCH DIE LEICHTFERTIGKEIT DER MITARBEITER UND HACKERANGRIFFE BEDROHT ALS VOR DREI JAHREN

Davon geht für die IT-Sicherheit im Unternehmen eine (sehr) große Gefahr aus –



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6267 (Juni / Juli 2013), 7251 (September 2016)

Schaubild 38

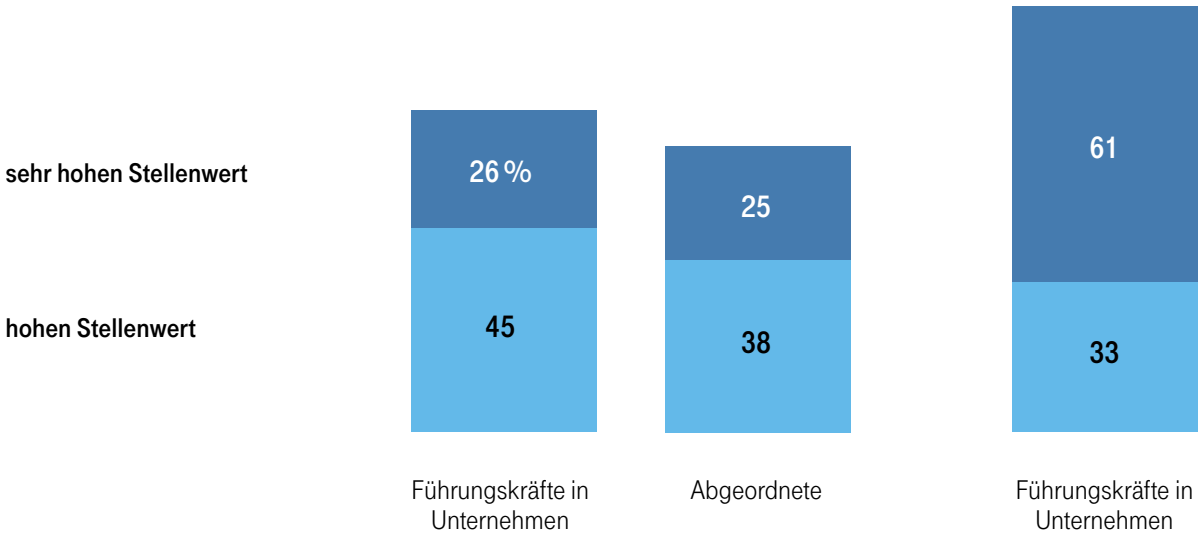
Dabei hat sich die Risikowahrnehmung in den letzten drei Jahren deutlich verändert. So ist heute ein jeweils deutlich größerer Anteil der Führungskräfte in der Wirtschaft überzeugt, dass für die IT-Sicherheit des eigenen Unternehmens (sehr) große Gefahr durch den leichtfertigen Umgang von Mitarbeitern mit Daten sowie durch Hackerangriffe auf das Unternehmen droht. Der Anteil derer, die (sehr) große Gefahren durch die Nutzung mobiler Endgeräte wie Smartphones und Tablet-PCs sehen, ist dagegen – trotz der zunehmenden Verbreitung dieser Geräte – von 50 Prozent auf 44 Prozent zurückgegangen (Schaubild 38).

DER SCHUTZ MOBILER ENDGERÄTE IST WICHTIG, ABER NICHT PRIORITÄR

Frage: „Welchen Stellenwert hat bei Ihnen im Unternehmen / Parlament der Schutz mobiler Endgeräte wie Smartphones und Tablets vor Zugriffen von außen?“

Der Schutz mobiler Endgeräte vor Zugriffen von außen hat einen –

Stellenwert der **IT-Sicherheit** im Unternehmen, also Schutz des Unternehmensnetzwerks vor Zugriffen von außen



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 39

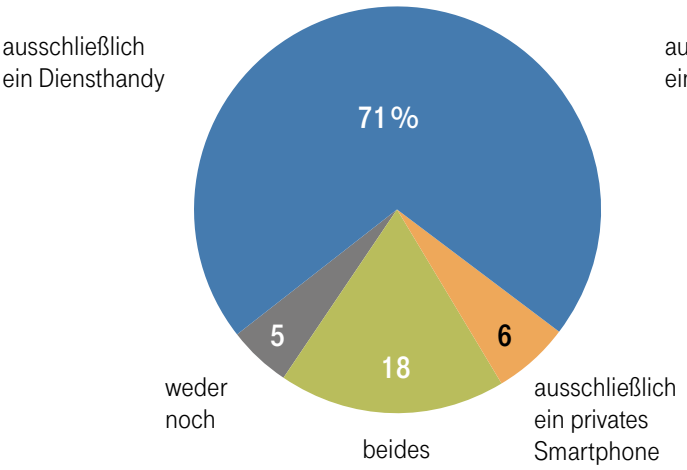
Dass die Gefahrenpotenziale mobiler Endgeräte heute niedriger eingeschätzt werden als noch vor drei Jahren, spiegelt sich auch darin wider, dass dem Schutz dieser Geräte vor Zugriffen von außen zwar ein hoher Stellenwert, aber offenbar keine Priorität eingeräumt wird. Nur in rund jeweils einem Viertel der Parlamente und mittleren und großen Unternehmen hat der Schutz mobiler Endgeräte einen sehr hohen Stellenwert.

Im Vergleich dazu genießt IT-Sicherheit ganz allgemein in 61 Prozent der mittleren und großen Unternehmen einen sehr hohen Stellenwert (Schaubild 39).

ABGEORDNETE NUTZEN ÜBERWIEGEND EIN PRIVATES SMARTPHONE FÜR DIENSTLICHE ANGELEGENHEITEN

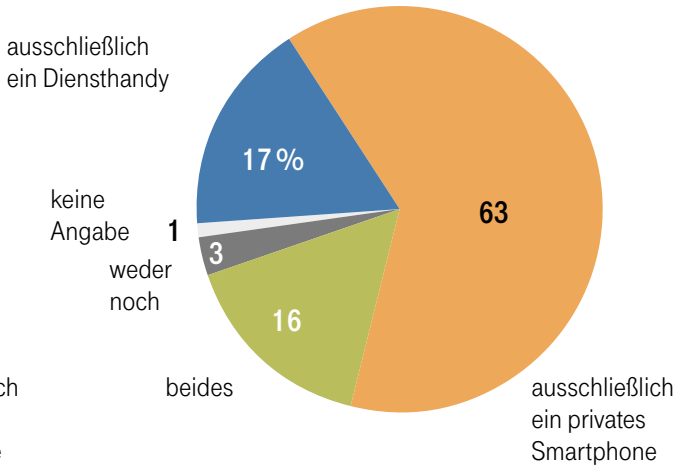
Frage: „Haben Sie selbst ein Diensthandy oder nutzen Sie ein privates Smartphone für geschäftliche/dienstliche Angelegenheiten oder beides?“

Für geschäftliche Angelegenheiten nutzen –



Führungskräfte in Unternehmen

Für dienstliche Angenheiten nutzen –



Abgeordnete

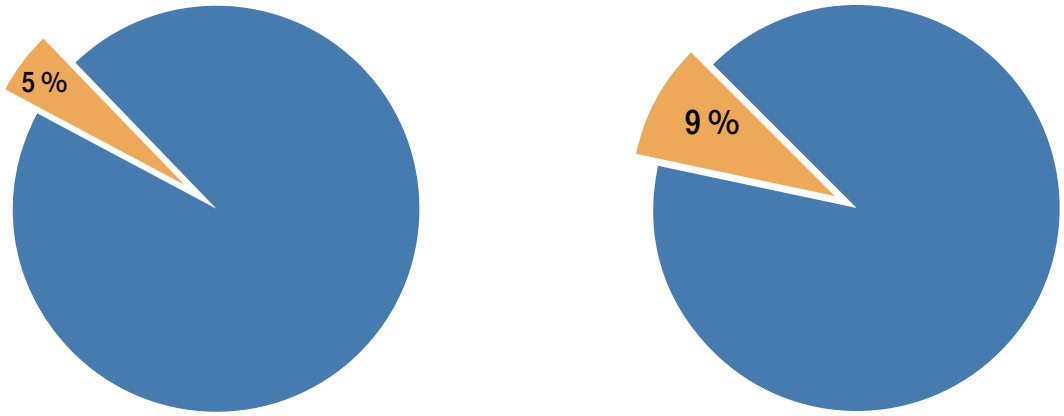
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 40

Während Führungskräfte aus der Wirtschaft für geschäftliche Angelegenheiten „nur“ zu rund einem Viertel (auch) ein privates Smartphone und ganz überwiegend ausschließlich ein Diensthandy nutzen (71 Prozent), ist das bei Abgeordneten deutlich anders: Sie nutzen zu fast zwei Dritteln ausschließlich ein privates Smartphone für dienstliche Angelegenheiten, weitere 16 Prozent sowohl ein Diensthandy als auch ein privates Smartphone (Schaubild 40).

NUR EIN KLEINER TEIL DER ENTSCHEIDER BERICHTET VON CYBER-ATTACKEN AUF IHR DIENSTLICH GENUTZTES HANDY

Das Smartphone bzw. Diensthandy wurde schon mal durch eine Cyber-Attacke angegriffen



die ein Diensthandy und/oder ein privates Smartphone für geschäftliche/dienstliche Angelegenheiten nutzen

Basis: Bundesrepublik Deutschland: Abgeordnete und Führungskräfte in Unternehmen, die entweder ein Diensthandy oder ein privates Smartphone bzw. beides besitzen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

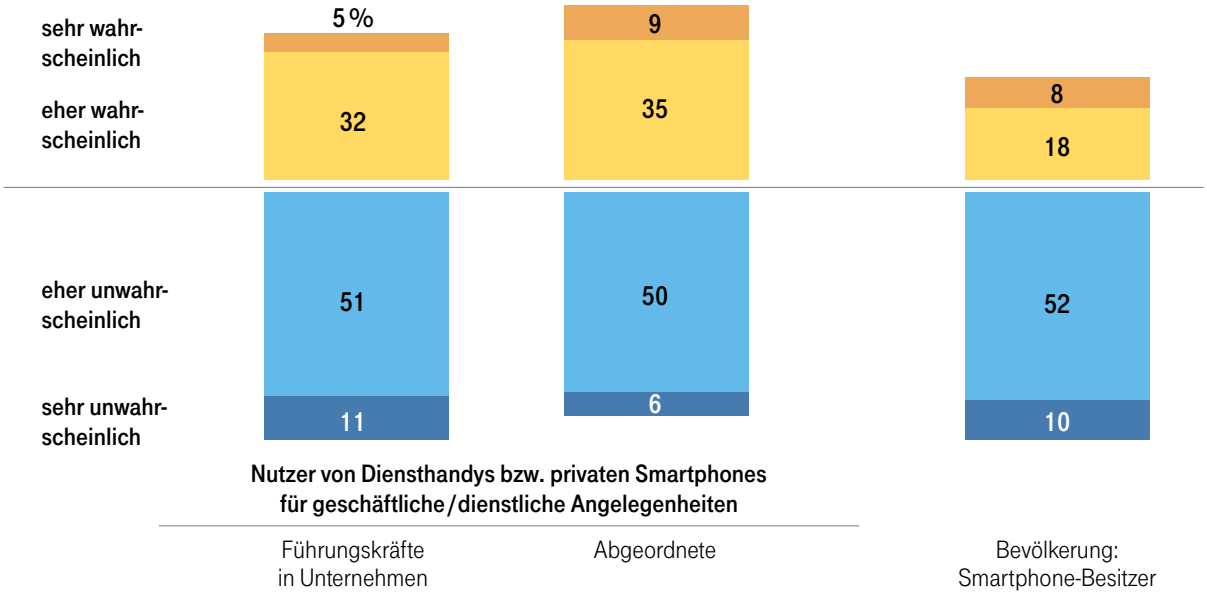
Schaubild 41

Von Cyber-Attacken auf ihr dienstlich genutztes Smartphone – sei es ein privates Gerät oder ein Diensthandy – berichtet nur eine Minderheit der Top-Entscheider: von den Führungskräften in mittleren und großen Unternehmen 5 Prozent, von den Abgeordneten immerhin 9 Prozent (Schaubild 41).

EINE CYBER-ATTACKE AUF DAS EIGENE SMARTPHONE WIRD VON VIELEN ENTSCHEIDERN ABER FÜR DURCHAUS WAHRSCHEINLICH GEHALTEN

Frage: „Für wie wahrscheinlich halten Sie es, dass Ihr Smartphone bzw. Diensthandy (noch einmal) durch eine Cyber-Attacke angegriffen wird?“

Ein Angriff auf das eigene Smartphone bzw. Diensthandy durch eine Cyber-Attacke halten für –



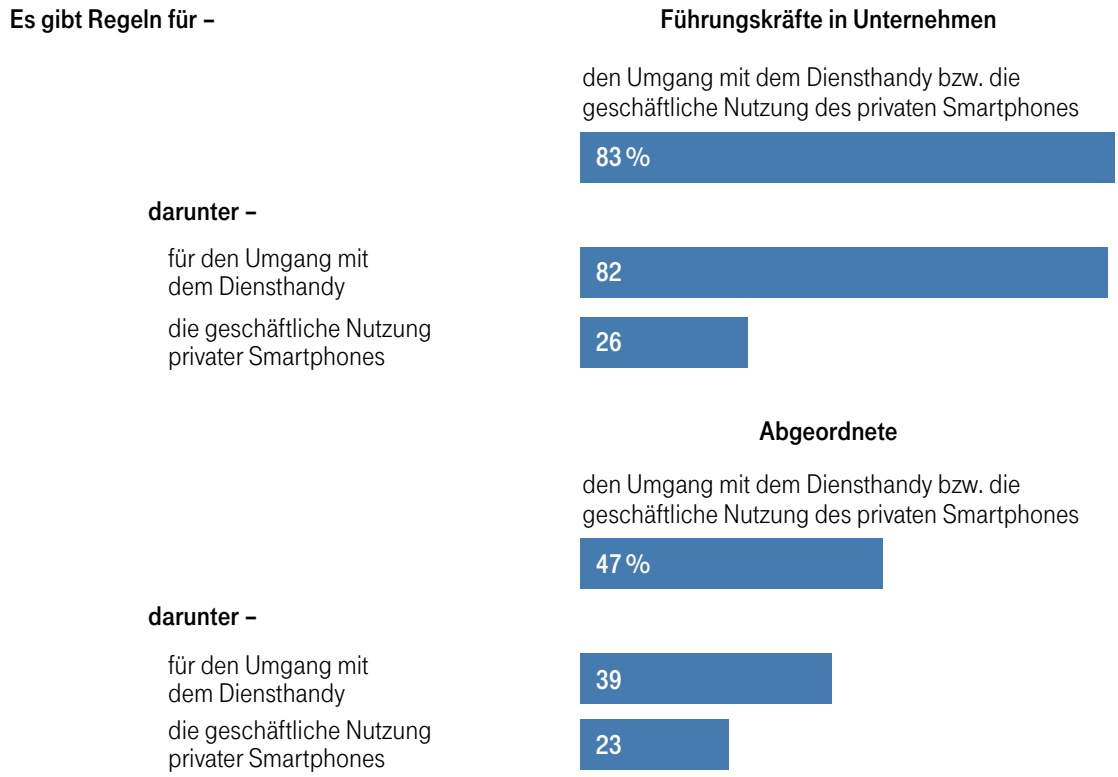
Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Bevölkerung ab 16 Jahren, Nutzer von Diensthandys bzw. privaten Smartphones für geschäftliche/dienstliche Angelegenheiten
Quelle: Allensbacher Archiv, IfD-Umfragen 11059 (August 2016), 7251 (September 2016)

Schaubild 42

Ein deutlich größerer Anteil hält eine Cyber-Attacke auf das eigene Smartphone aber für durchaus wahrscheinlich: 37 Prozent der Führungskräfte in Unternehmen, die ein solches Gerät geschäftlich nutzen, und 44 Prozent der Abgeordneten schätzen dies als eher oder sogar sehr wahrscheinlich ein. Eine jeweilige Mehrheit hält das dagegen für eher oder sehr unwahrscheinlich. Dennoch stufen die Entscheider aus Politik und Wirtschaft die Gefahr einer Cyber-Attacke auf das eigene Smartphone damit größer ein als die Smartphone-Besitzer in der Bevölkerung insgesamt (Schaubild 42).

BEI ABGEORDNETEN GIBT ES HÄUFIG KEINE REGELN ZUM UMGANG MIT DEM DIENSTHANDY BZW. DEM PRIVAT GENUTZTEN SMARTPHONE



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 43

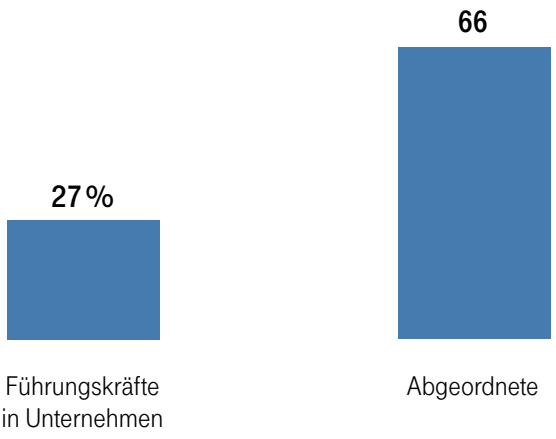
Angesichts der insbesondere unter Abgeordneten verbreiteten Überzeugung, dass eine Cyber-Attacke auf das eigene Smartphone wahrscheinlich ist, erstaunt, wie häufig den Abgeordneten keine schützenden Regeln an die Hand gegeben werden. Nur 47 Prozent der Abgeordneten berichten davon, dass es für die dienstliche Nutzung von Smartphones Regeln gibt, darunter bei 39 Prozent Regeln für den Umgang mit dem Diensthandy und bei 23 Prozent Regeln für die geschäftliche Nutzung des privaten Smartphones – dabei nutzen rund vier von fünf Abgeordneten (auch) ein privates Smartphone für dienstliche Angelegenheiten.[5]

Für mittlere und große Unternehmen berichten immerhin 82 Prozent der Führungskräfte von Regeln für die Nutzung von Diensthandys, weitere 26 Prozent von Regeln für die geschäftliche Nutzung des privaten Smartphones (Schaubild 43).

[5] Vgl. Schaubild 40, Seite 45.

RUND ZWEI DRITTEL DER ABGEORDNETEN NUTZEN FÜR DIENSTLICHE ANGELEGENHEITEN EIN SMARTPHONE, OHNE DASS ES DAFÜR REGELN GIBT

Es nutzen ein Diensthandy oder ein privates Smartphone für geschäftliche/dienstliche Angelegenheiten, ohne dass es für diese Nutzung Regeln gibt –



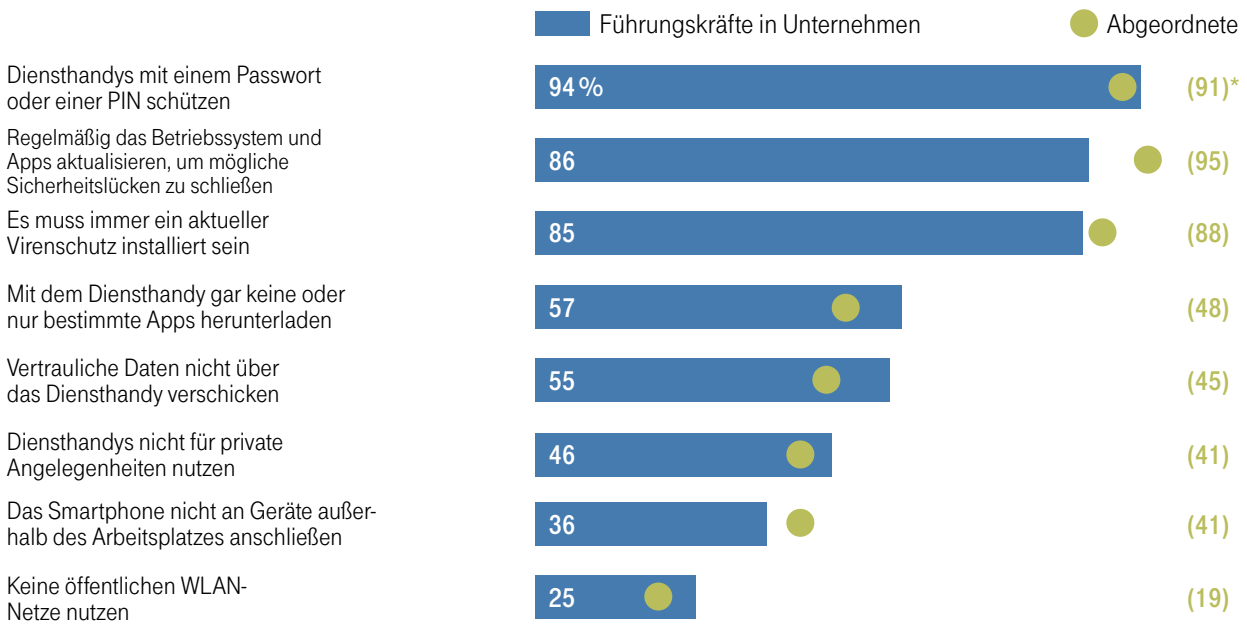
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 44

Insgesamt nutzen zwei Drittel der Abgeordneten ein Diensthandy oder ein privates Smartphone für dienstliche Angelegenheiten, ohne dass es für diese Nutzung Regeln zum Schutz vor Zugriffen von außen gibt. Bei den Führungskräften aus der Wirtschaft ist dieser Anteil deutlich kleiner, mit 27 Prozent aber immer noch bemerkenswert (Schaubild 44).

REGELN FÜR DEN UMGANG MIT DEM DIENSTHANDY

Es gibt die Regel –



*( ) Wegen geringer Fallzahl (n = 42) nur als Tendenzbefund zu interpretieren.

Basis: Bundesrepublik Deutschland: Abgeordnete und Führungskräfte in Unternehmen, bei denen es Regeln für die Nutzung von Diensthandys gibt

Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

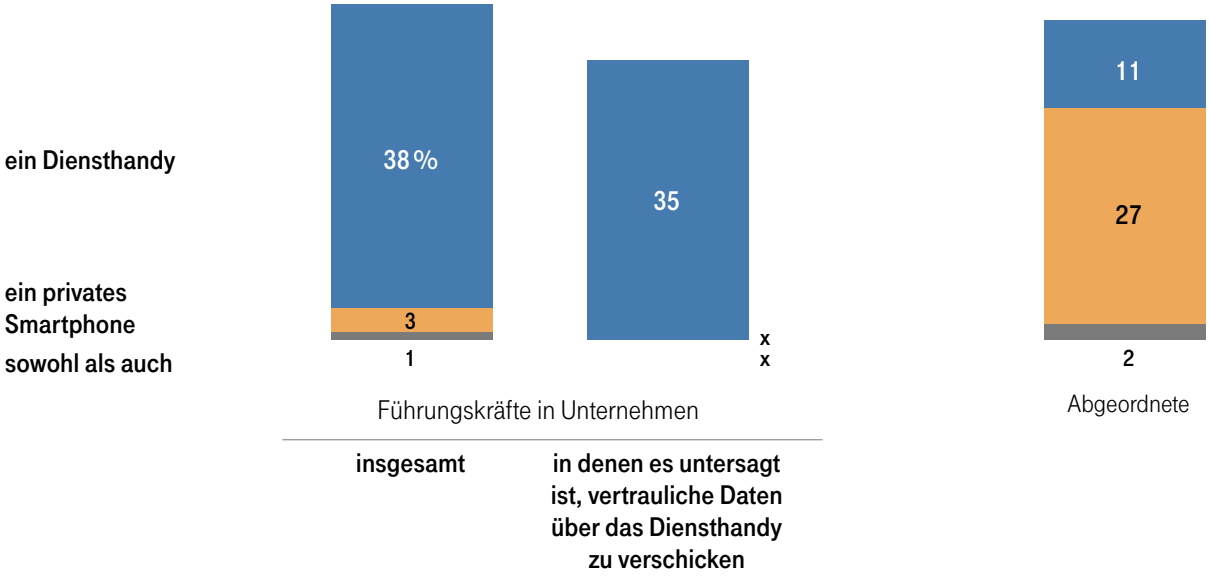
Schaubild 45

Sofern Regeln für die Nutzung eines Diensthandys bestehen, sind es vor allem drei Regeln, die sowohl für Wirtschaftsführer als auch für Abgeordnete sehr verbreitet gelten: dass das Diensthandy mit einem Passwort oder einer PIN zu schützen ist, dass Betriebssystem und Apps regelmäßig aktualisiert werden müssen, um mögliche Sicherheitslücken zu schließen, und dass immer ein aktueller Virenschutz installiert sein muss (jeweils 85 Prozent oder mehr). In 57 Prozent der mittleren und großen Unternehmen dürfen mit einem Diensthandy nur bestimmte oder gar keine Apps heruntergeladen werden[6], in 55 Prozent der Unternehmen keine vertraulichen Daten über das Diensthandy verschickt werden. Diese beiden Regeln gelten auch für jeweils rund die Hälfte der Abgeordneten. Öffentliche WLAN-Netzte zu benutzen untersagt nur jedes vierte Unternehmen (Schaubild 45). Von den insgesamt 8 abgefragten möglichen Regeln zum Schutz eines Diensthandys gelten in Unternehmen im Durchschnitt 4,8, d. h., gut 3 dieser Regeln gelten im Durchschnitt nicht.

[6]Darunter dürfen in 46 Prozent der Unternehmen nur bestimmte, in 11 Prozent gar keine Apps auf das Diensthandy geladen werden (vgl. tabellarischer Basisbericht).

VIELE ENTSCHEIDER NUTZEN EIN SMARTPHONE, UM VERTRAULICHE DOKUMENTE ZU EMPFANGEN ODER ZU VERSENDEN

Um sich vertrauliche (geschäftliche) Daten oder Dokumente schicken zu lassen oder selbst zu versenden, nutzen –



x = unter 0,5 Prozent

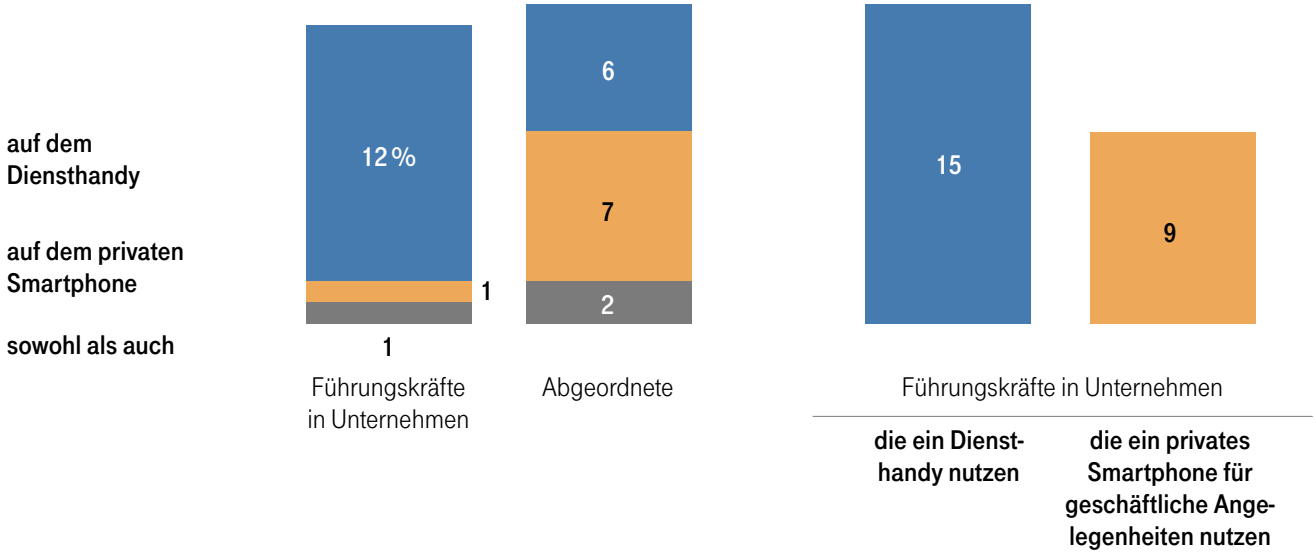
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 46

Zudem helfen Regeln wenig, wenn sie von den Nutzern missachtet werden. So nutzen insgesamt 42 Prozent der Führungskräfte aus Unternehmen ihr Diensthandy oder ein privates Smartphone, um sich vertrauliche geschäftliche Daten oder Dokumente schicken zu lassen oder selbst zu verschicken. In Unternehmen, in denen es untersagt ist, vertrauliche Daten über das Diensthandy zu verschicken, ist dieser Anteil nicht sehr viel kleiner: Von den Führungskräften dort nutzen immerhin 35 Prozent das Diensthandy, um sich vertrauliche geschäftliche Daten oder Dokumente schicken zu lassen oder selbst zu verschicken. Abgeordnete nutzen ihr Diensthandy oder privates Smartphone in insgesamt ähnlichem Umfang zum Empfang oder Versand vertraulicher Daten oder Unterlagen (Schaubild 46).

RUND JEDER SIEBTE ENTSCHEIDER SPEICHERT VERTRAULICHE DATEN AUF DEM SMARTPHONE

Es speichern vertrauliche (geschäftliche) Daten oder Dokumente –



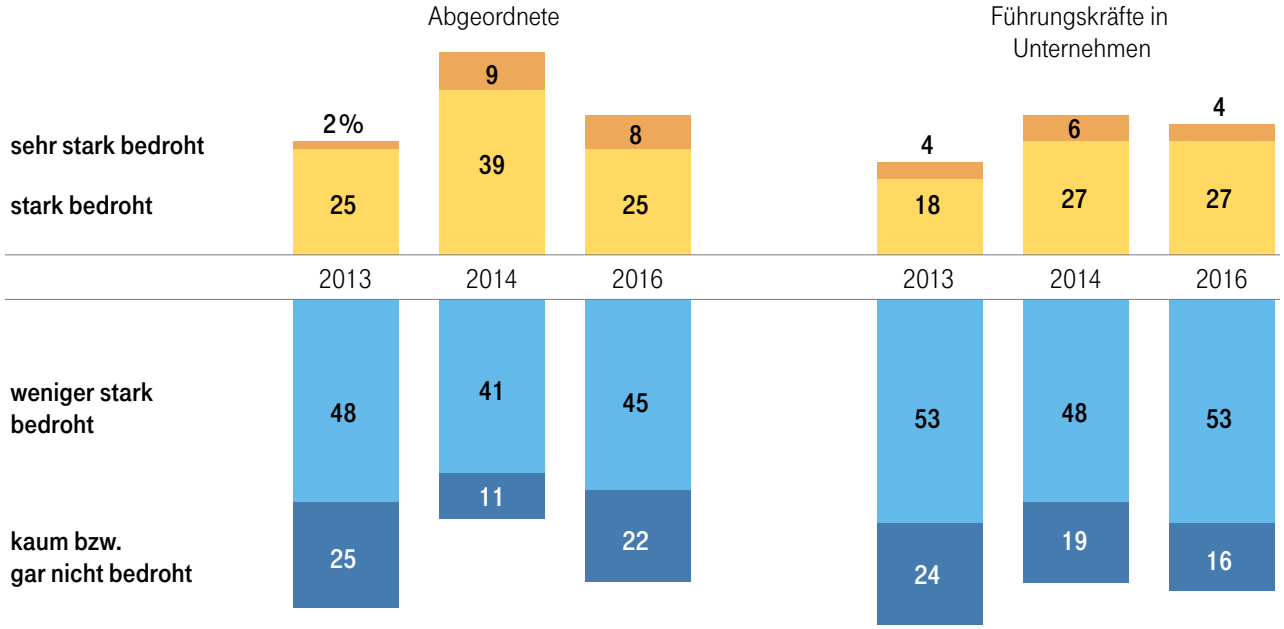
Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 7251 (September 2016)

Schaubild 47

Der Anteil der Führungskräfte, die vertrauliche Daten oder Dokumente auf ihrem Smartphone speichern, ist demgegenüber zwar kleiner, dennoch aber bemerkenswert groß. So speichert insgesamt rund jeder siebte Entscheider aus mittleren und großen Unternehmen bzw. etwa jeder siebte Abgeordnete Vertrauliches auf seinem Diensthandy und/oder privaten Smartphone. Unter den Wirtschaftsführern, die (auch) ein privates Smartphone für geschäftliche Angelegenheiten nutzen, legen 9 Prozent dort auch vertrauliche Daten oder Dokumente ab (Schaubild 47).

DAS PERSÖNLICHE BEDROHUNGSGEFÜHL DURCH IT-ANGRIFFE HAT NICHT WEITER ZUGENOMMEN

Frage: „Wie stark fühlen Sie sich persönlich durch IT-Angriffe bedroht, also dass z. B. Ihr Smartphone oder Ihr Computer gehackt werden oder dass sich jemand mit Ihren Passwörtern Zugang zu Ihren persönlichen oder unternehmensinternen Daten verschafft? Würden Sie sagen, Sie fühlen sich ...“



Auf 100 fehlende Prozent: Unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfragen 6267 (Juni / Juli 2013), 6289 (September 2014) und 7251 (September 2016)

Schaubild 48

Dass sowohl beim Cloud Computing als auch bei der Verschlüsselung von geschäftlichen bzw. dienstlichen E-Mails und der Nutzung von Smartphones die Sicherheitsbedenken bzw. die Einsicht in die Risikopotenziale nur zum Teil in entsprechende Handlungen münden, mag auch damit zusammenhängen, dass das persönliche Bedrohungsgefühl bei einer Mehrheit der Führungskräfte eher gering ist. Jeweils nur rund ein Drittel der Abgeordneten und der Wirtschaftsführer fühlt sich persönlich durch IT-Angriffe z. B. auf das eigene Smartphone oder den eigenen Computer (sehr) stark bedroht. Jeweils rund zwei Drittel fühlen sich dagegen weniger stark oder gar nicht bedroht. Bei Abgeordneten war dieses Bedrohungsgefühl 2014 schon einmal deutlich ausgeprägter – vermutlich unter dem Eindruck der Enthüllungen um von der NSA abgehörte Handys von Politikern. Bei Wirtschaftsführern ist das persönliche Bedrohungsgefühl durch Cyber-Angriffe gegenüber 2014 nicht gewachsen, bei Abgeordneten auch im Vergleich zu 2013 nur leicht (Schaubild 48).

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

ERLEBEN, WAS VERBINDET.