

Cyber Security Report 2013

Ergebnisse einer repräsentativen Befragung
von Abgeordneten sowie Führungskräften in mittleren
und großen Unternehmen



INHALT

VORWORT	4
VORBEMERKUNGEN	5
IT- UND DATENSICHERHEIT ALS GROSSE GESELLSCHAFTLICHE RISIKEN	6
BIG DATA – ENTSCHIEDER SEHEN EHER RISIKEN ALS NUTZEN FÜR DIE VERBRAUCHER	13
HOHER STELLENWERT DER IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN	17
GEFAHRENQUELLEN UND HERAUSFORDERUNGEN IM BEREICH IT-SICHERHEIT – VERHALTEN DER MITARBEITER ALS GRÖSSTES RISIKO	30
IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN	35
UNTERNEHMENSÜBERGREIFENDE INITIATIVEN WERDEN FÜR WICHTIG GEHALTEN – BISLANG IST ABER NUR EINE MINDERHEIT DER UNTERNEHMEN IN INITIATIVEN ZUM THEMA IT-SICHERHEIT EINGEBUNDEN	45
ANHANG: STUDIENDESIGN IM ÜBERBLICK	52

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

VORWORT

Die globalen Überwachungs- und Spähpraktiken von Geheimdiensten sind noch lange nicht aufgeklärt. Doch die Folgen von PRISM und Tempora zeichnen sich bereits deutlich ab – das zeigt der jetzt vorliegende Cyber Security Report. Das gesellschaftliche Risikopotenzial von Cyberangriffen, Wirtschaftsspionage und Datenmissbrauch wird von einer Mehrheit der befragten Abgeordneten und Spitzenführungskräfte deutscher Unternehmen sehr hoch eingestuft. Aus ihrer Sicht sind die Gefahren aus dem und über das Netz im Vergleich zum Vorjahr nochmals beträchtlich gestiegen. Vor allem die Sorge im Hinblick auf eine Überwachung der Bürger durch den Staat beunruhigt: Jeder Vierte bewertet das Ausspähen von Telefon- oder Internetdaten als Risiko für die Gesellschaft.

Trotz der berechtigten Empörung über die Vorgehensweise sollten wir auch die „guten“ Seiten dieses staatlich verordneten Datenmissbrauchs sehen. Die Enthüllungen des amerikanischen Whistleblowers Edward Snowden haben allen deutlich gemacht: In einer digitalen Gesellschaft sind personenbezogene Daten und jede für ein Unternehmen oder einen Staat wichtige Information ein äußerst wertvolles Gut. Diese Werte müssen wir gegen Missbrauch schützen – was angesichts einer zunehmenden digitalen Vernetzung nicht ganz einfach ist. PRISM und Tempora sind durch das breite und teils rücksichtslose Abgreifen von Daten in ihrer Dimension kaum zu überbieten. Gefahren lauern im Netz aber überall. Deutsche Verfassungsschützer gehen davon aus, dass eine ganze Reihe von Regierungen und Unternehmen professionelle Hacker gezielt mit Wirtschaftsspionage beauftragt. Hacker bieten ihre Dienste inzwischen im Internet an oder – ganz dreist – auf Messen. Dazu kommen die Angreifer, die einfach nur Schaden verursachen wollen. Fast täglich berichten die Medien über erfolgreiche Angriffe von Cyberkriminellen auf Netzwerke von Unternehmen. Laut dieser Allensbach-Studie ist die überwiegende Zahl der Unternehmen IT-Angriffen ausgesetzt, zwölf Prozent sind es

täglich. Wie lautet Konsequenz? Stecker ziehen und zurück ins analoge Zeitalter? Das will niemand. Aber wir alle – Unternehmen, Staat und Privatpersonen – müssen uns mit aller Konsequenz gegen Cyberangriffe und Datenmissbrauch schützen. Und besonders wir Unternehmen sollten den Verlockungen der so wertvollen Daten widerstehen und vor allem mit den personenbezogenen Daten konsequent verantwortlich umgehen. Das sehen mehr als zwei Drittel der für diese Studie Befragten genauso: Sie bewerten die Speicherung von Kundendaten, das Abgreifen von personenbezogenen Informationen aus den Social-Media-Kanälen und deren Analyse für die Verbraucher als hohes Risiko. Sie halten daher strengere gesetzliche Vorgaben bei der Speicherung und Verwendung von Kundendaten für sinnvoll.

Staat und Wirtschaft sind indes auch bei der Abwehr von Cyberwar und Wirtschaftsspionage gefragt. Immerhin schätzt mehr als die Hälfte der Großunternehmen das Schadensrisiko durch einen Hackerangriff als groß bis sehr groß ein. Deshalb besteht bei den meisten Führungskräften und Abgeordneten weitgehend Einigkeit: Die Priorität der Politik im Bereich IT-Sicherheit muss auf dem Schutz der kritischen physischen Infrastrukturen liegen. Danach folgt eine stärkere internationale Zusammenarbeit und schließlich eine erhöhte Sensibilisierung und Aufklärung der Bürger beim Umgang mit Computer und Internet.

Die Aufgaben sind nicht einfach. Sie lassen sich nur gemeinsam bewältigen. Aus diesem Grund brauchen wir mehr Transparenz und eine übergreifende koordinierte Vorgehensweise, um uns gegen Cyberkriminelle nachhaltig zu schützen.

Reinhard Clemens
Vorstand Deutsche Telekom und CEO T-Systems

VORBEMERKUNGEN

„Cyber Security“ wird für Unternehmen wie für die Politik immer mehr zu einem kritischen Thema. Daher hat das INSTITUT FÜR DEMOSKOPIE ALLENSBACH im Auftrag von T-SYSTEMS sowie in Kooperation mit dem CENTRUM FÜR STRATEGIE UND HÖHERE FÜHRUNG nach 2011 und 2012 zum dritten Mal Entscheider aus Politik und Wirtschaft nach ihrer allgemeinen Risikoeinschätzung sowie zu ausgewählten Themen im Bereich „Cyber Security“ befragt.

Mit Blick auf IT- und Cybersicherheit lag der Schwerpunkt der Studie dabei zum einen auf Chancen und Risiken von Big Data, dem Stellenwert der IT-Sicherheit im eigenen Unternehmen sowie Gefahrenquellen und Handlungsbedarf für Unternehmen im Bereich IT-Sicherheit. Zum anderen wurden die Erwartungen an Politik und Behörden, die Bewertung der staatlichen Fachkompetenz im Bereich IT-Sicherheit sowie die Bedeutung unternehmensübergreifender Initiativen für IT-Sicherheit untersucht.

Die Studie stützt sich auf insgesamt 631 Interviews mit einem repräsentativen Querschnitt von Politikern und Führungskräften in mittleren und großen Unternehmen. Die Interviews wurden zwischen dem 5. Juni und 15. Juli 2013 telefonisch durchgeführt. Als Entscheider aus der Politik wurden 117 Abgeordnete aus Bundestag, Landtagen und deutsche Abgeordnete aus dem Europaparlament befragt. Bei den Führungskräften aus

der Wirtschaft wurden insgesamt 514 Führungskräfte aus großen und mittleren Unternehmen befragt, darunter 221 Führungskräfte aus großen Unternehmen und 293 Führungskräfte aus mittleren Unternehmen. Zu den großen Unternehmen zählen gemäß Definition der EU-Kommission Unternehmen mit mindestens 250 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 nur rund 2 Prozent aller Unternehmen in Deutschland, erwirtschaften allerdings rund 80 Prozent aller umsatzsteuerpflichtigen Waren und Dienstleistungen und beschäftigen etwa zwei Drittel aller sozialversicherungspflichtig Beschäftigten in Deutschland.

Führungskräfte aus mittleren Unternehmen wurden in diesem Jahr erstmals befragt. Daher beziehen sich Vergleiche mit Ergebnissen aus den Vorjahren nur auf Führungskräfte aus großen Unternehmen bzw. Abgeordnete und Führungskräfte aus großen Unternehmen.

(INSTITUT FÜR DEMOSKOPIE ALLENSBACH)

IT- UND DATENSICHERHEIT ALS GROSSE GESELLSCHAFTLICHE RISIKEN

Aus Sicht der Entscheider aus Politik und Wirtschaft stellen Cybergefahren und Datenschutzverletzungen unter 22 Risiken aus allen Lebensbereichen das größte Risikopotenzial für die Bevölkerung in Deutschland dar. Unter den sechs größten Risiken finden sich vier wieder, die mit IT- und Datensicherheit zusammenhängen: 62 Prozent der Entscheider sehen im Datenbetrug im Internet ein großes Risiko für die Menschen in Deutschland. Für genauso viele stellt der Missbrauch persönlicher Daten durch andere Nutzer sozialer Netzwerke ein großes gesellschaftliches Risiko dar. 57 Prozent sehen in Computerviren, 50 Prozent im Missbrauch persönlicher Daten durch Unternehmen ein großes Risiko für die Bevölkerung. Mindestens eine der vier genannten Gefahren sehen 87 Prozent der Entscheider als großes Risiko an. Eine andere Facette der IT- und Datensicherheit ist die staatliche Überwachung der Bürger, insbesondere der Internet- oder Telefonverbindungen. 27 Prozent der Entscheider sehen darin ein großes Risiko für die Menschen in Deutschland. Im Vergleich zu den einzelnen

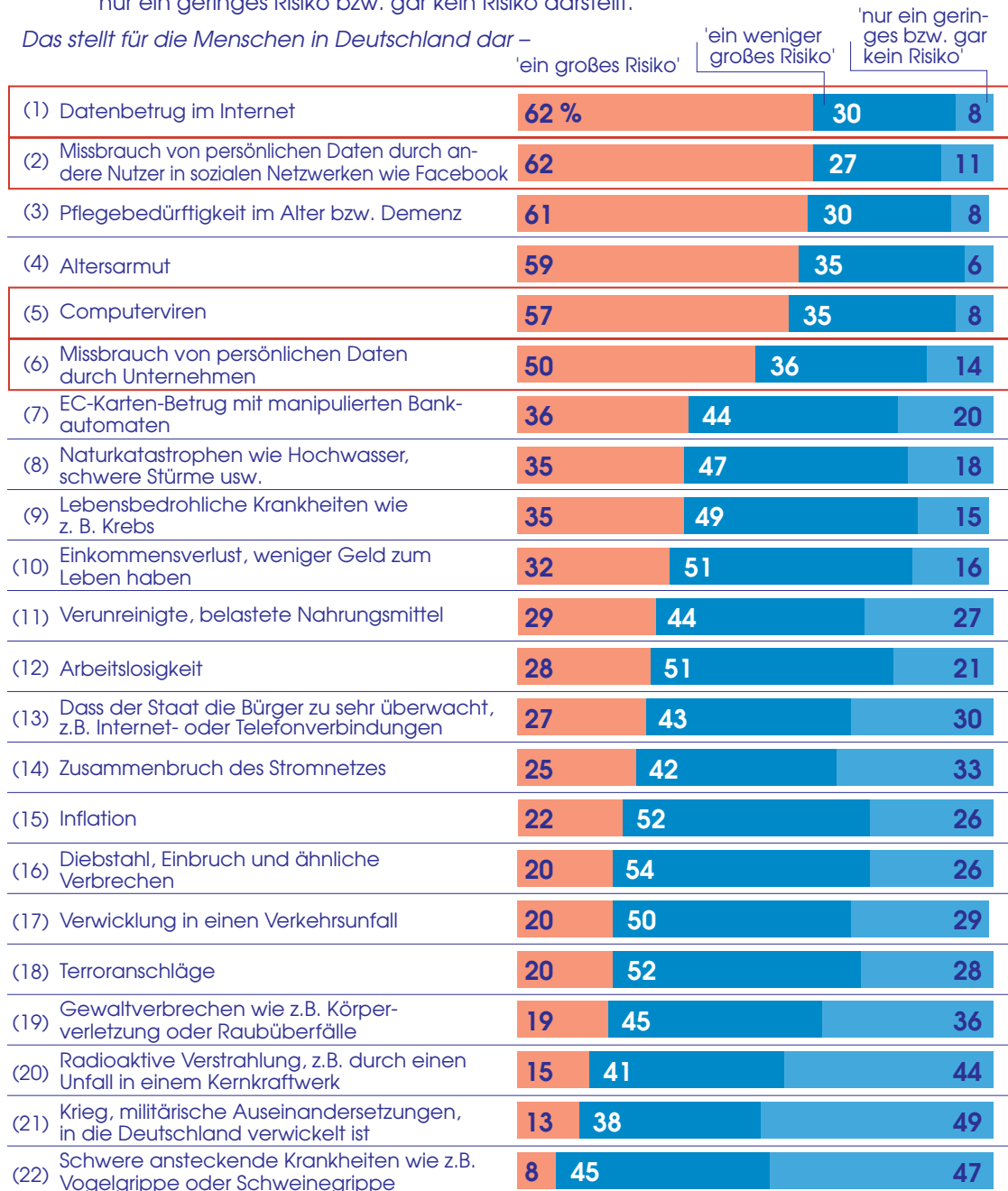
IT- und Datenrisiken werden von den Politikern und Führungskräften in mittleren und großen Unternehmen nur Altersrisiken als ähnlich bedeutsam eingestuft: So sehen 61 Prozent der Entscheider die Pflegebedürftigkeit im Alter, 59 Prozent das Thema Altersarmut als großes Risiko für die Bevölkerung an.

Andere Risiken folgen erst mit deutlichem Abstand: Der EC-Karten-Betrug mit manipulierten Bankautomaten, der im weitesten Sinne noch zu den IT-Gefahren gezählt werden kann, stellt für 36 Prozent der Entscheider ein großes Risiko dar. Naturkatastrophen folgen mit 35 Prozent. Für ebenso viele Abgeordnete und Führungskräfte aus der Wirtschaft gelten lebensbedrohliche Krankheiten wie Krebs als großes gesellschaftliches Risiko. Materielle Risiken wie Einkommensverlust, Arbeitslosigkeit und Inflation spielen mit 32, 28 bzw. 22 Prozent aus Sicht der Entscheider eine eher nachrangige Rolle. Auch ein Zusammenbruch des Stromnetzes gilt nur jedem vierten Entscheider als großes Risiko (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 dar –



Auf 100 fehlende Prozent: unentschieden

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

Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT- UND DATENSICHERHEIT ALS GROSSE GESELLSCHAFTLICHE RISIKEN

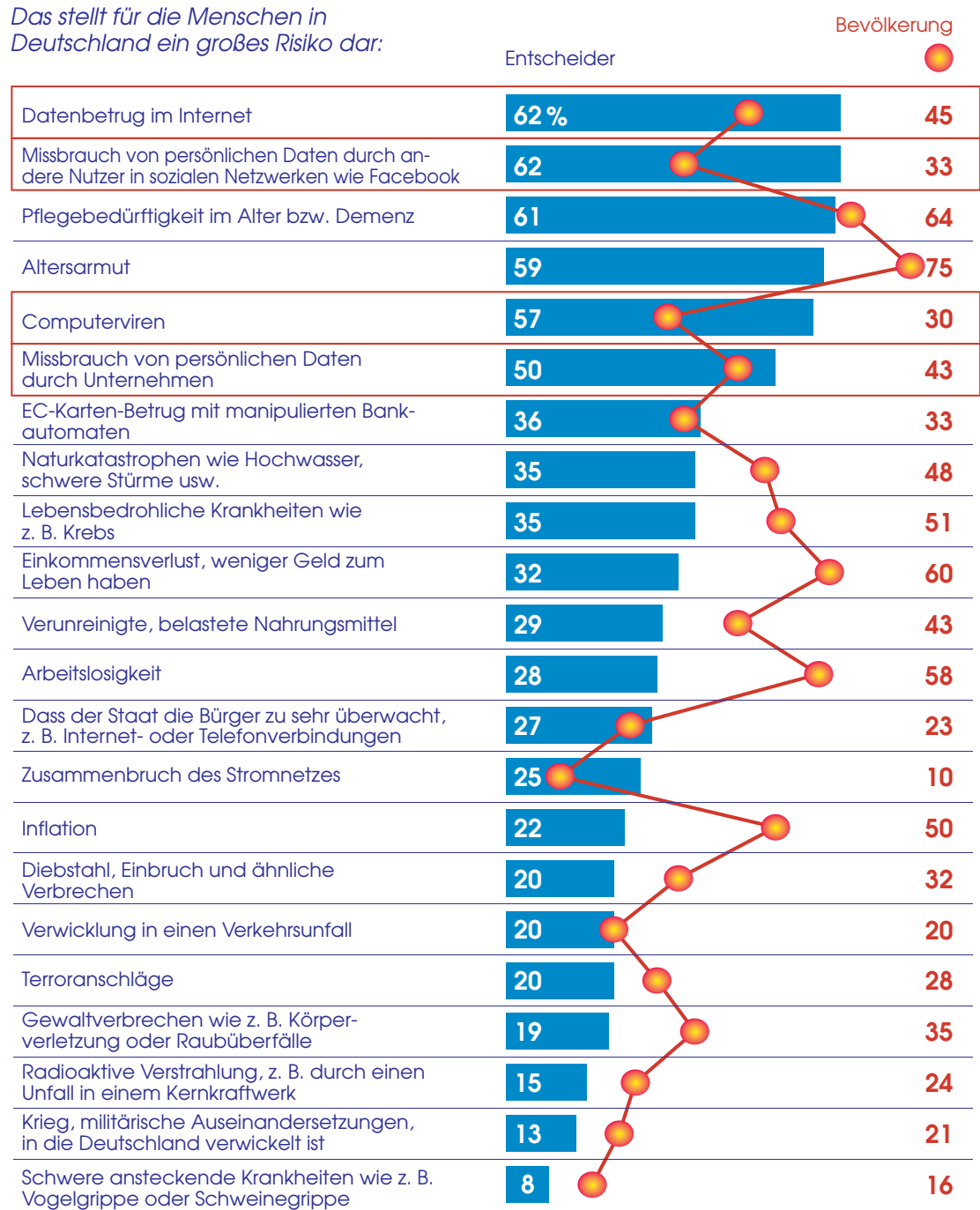
Entscheider stufen das gesellschaftliche Risikopotenzial von Cyber- und Datenrisiken damit deutlich höher ein, als dies die Bevölkerung tut. Das zeigt der direkte Vergleich der Einschätzungen von Entscheidern und Bevölkerung. So sehen beispielsweise 45 Prozent der Bürger im Datenbetrug im Internet ein großes gesellschaftliches Risiko; bei den Entscheidern sind es 62 Prozent. Und auch die anderen Cyber- und Datenrisiken – Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken, Computerviren und der Missbrauch von persönlichen Daten durch Unternehmen – werden von den Entscheidern aus Politik und Wirtschaft als weitaus relevanter

eingestuft als von der Bevölkerung. Mindestens eine der vier Gefahren bewerten 68 Prozent der Bevölkerung, aber 87 Prozent der Entscheider – als großes gesellschaftliches Risiko ein.

Die Bevölkerung sieht im Vergleich zu den Entscheidern aus Politik und Wirtschaft dagegen insbesondere in materiellen Risiken wie Altersarmut, Einkommensverlust, Arbeitslosigkeit oder Inflation – ebenso wie in gesundheitlichen Risiken – eine größere Bedrohung für die Menschen in Deutschland (Schaubild 2).

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 11009 und 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT- UND DATENSICHERHEIT ALS GROSSE GESELLSCHAFTLICHE RISIKEN

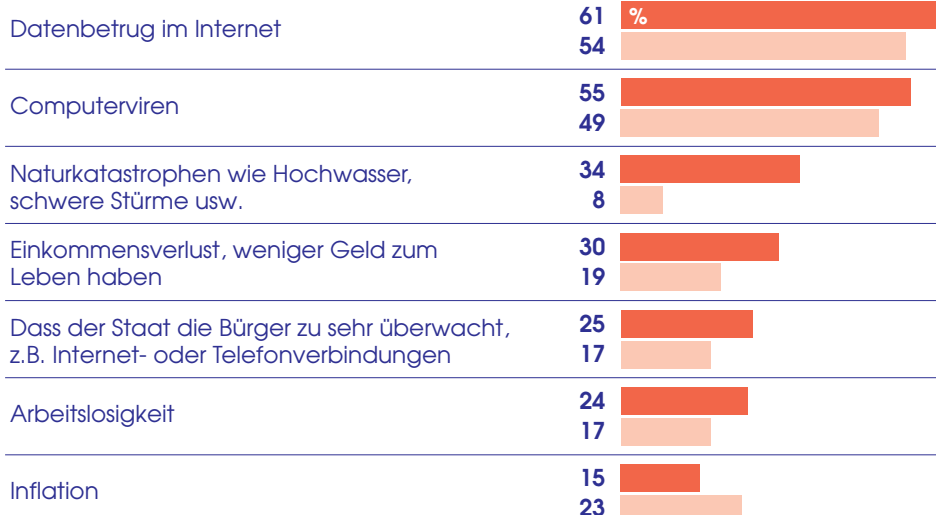
Im Vergleich zum Vorjahr ist aus Sicht der Entscheider die Gefahr durch Cyber- und Datenrisiken gestiegen. So betrachteten vor einem Jahr 54 Prozent der Abgeordneten und Führungskräfte aus großen Unternehmen – nur für diese Gruppe ist ein Vergleich mit dem Vorjahr möglich – den Datenbetrug im Internet als großes gesellschaftliches Risiko, heute sind es 61 Prozent. Die Sicherheitsgefährdung, die von Computerviren ausgeht, wird mit 55 Prozent ebenfalls etwas höher eingestuft als im Vorjahr, als 49 Prozent dieser Entscheider darin ein großes gesellschaftliches Risiko sahen.¹ Deutlich gestiegen ist im Vergleich zum Vorjahr die Einschätzung, dass die staatliche Überwachung der Bürger, vor allem ihrer Telefon- und Internetverbindungen, ein gesellschaftliches Risiko darstellt. Vor einem Jahr sahen 17 Prozent der Abgeordneten und Führungskräfte aus großen Unternehmen darin

ein großes gesellschaftliches Risiko. Heute sind es unter dem Eindruck der Medienberichterstattungen über die Aktivitäten der US-amerikanischen und britischen Geheimdienste zur Überwachung von Internet- und Kommunikationsinhalten in Deutschland 25 Prozent. Die größte Veränderung bei der Risikobewertung gab es angesichts der jüngsten Überschwemmungen in weiten Teilen Bayerns und Ostdeutschlands bei der Risikobewertung von Naturkatastrophen. 2012 sahen darin 8 Prozent der Abgeordneten und Führungskräfte aus großen Unternehmen ein relevantes Risiko, in diesem Jahr sind es 34 Prozent. Bei den materiellen Risiken zeigt sich ein uneinheitliches Bild: Einkommensverlust und Arbeitslosigkeit gelten stärker als noch vor einem Jahr als gesellschaftliche Risiken, das Inflationsrisiko wird dagegen als geringer eingestuft (Schaubild 3).

Schaubild 3

Gesellschaftliches Risikopotenzial von Cyber- und Datenrisiken hat aus Sicht der Entscheider zugenommen

Das stellt aus Sicht von Abgeordneten und Führungskräften in großen Unternehmen ein großes Risiko für die Menschen in Deutschland dar –
– Auswahl –



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6240 und 6267

© IfD-Allensbach

¹ Für die Risiken „Missbrauch von persönlichen Daten durch Unternehmen, z.B. dass persönliche Daten unerlaubt weitergegeben werden“ und „Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken wie Facebook“ ist kein Vergleich mit dem Vorjahr möglich. Die Items sind in diesem Jahr in dieser Form neu aufgenommen worden. Im Vorjahr wurde der Missbrauch persönlicher Daten in Form eines pauschalen Items („Missbrauch von persönlichen Daten, z.B. dass persönliche Daten unerlaubt weitergegeben werden“) abgefragt.

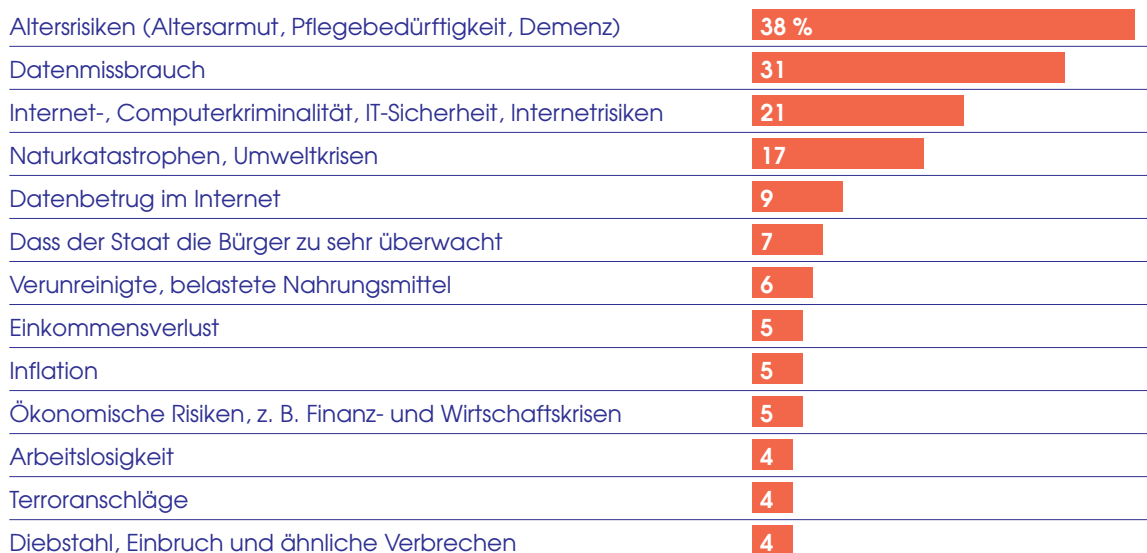
Die Entscheider aus Politik und Wirtschaft wurden nicht nur um ihre derzeitige Risikobewertung gebeten, sondern auch um eine Einschätzung, welche Risiken aus ihrer Sicht künftig besonders stark zunehmen werden. Da die Abfrage zur künftigen Risikoentwicklung als offene, ungestützte Frage (also ohne konkrete Antwortvorgaben) erfolgte, ist ein Vergleich der absoluten Werte mit der gegenwärtigen 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. 31 Prozent verweisen auf den Missbrauch von Daten als wachsende Gefahrenquelle, 21 Prozent auf Internet- und Computerkriminalität sowie die IT-Sicherheit generell. 9 Prozent rechnen mit einer besonders starken Zunahme von Datenbetrug im Internet.

55 Prozent der Entscheider erwarten, dass mindestens eines dieser drei Risiken künftig stark zunehmen wird. Damit werden aus Sicht von Abgeordneten und Führungskräften in der Wirtschaft IT- und Datenrisiken in Zukunft noch stärker zunehmen als Altersrisiken wie Altersarmut und Pflegebedürftigkeit, die nach Meinung von 38 Prozent der Entscheider stark anwachsen werden. Wie bereits bei der aktuellen Risikobewertung schlagen sich auch bei der Einschätzung der künftigen Risikoentwicklung die diesjährigen Überschwemmungen in weiten Teilen Bayerns und Ostdeutschlands nieder: 17 Prozent schreiben Naturkatastrophen und Umwelt Risiken ein stark steigendes Risikopotenzial zu. Andere Risiken spielen dagegen – bei der ungestützten Abfrage – eine eher untergeordnete Rolle (Schaubild 4).

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 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT- UND DATENSICHERHEIT ALS GROSSE GESELLSCHAFTLICHE RISIKEN

Politiker und Führungskräfte in den Unternehmen bewerten die künftige Risikoentwicklung weitgehend ähnlich. Deutliche Unterschiede gibt es im Wesentlichen nur bei der Bewertung der künftigen Entwicklung von Altersrisiken und Einkommensverlust. Beide Risiken werden aus Sicht von Politikern stärker ansteigen als nach Einschätzung der Führungskräfte aus der Wirtschaft. So gehen 52 Prozent der Politiker davon aus, dass Altersarmut, Pflegebedürftigkeit und Demenzerkrankungen künftig stark zunehmen werden, von den Führungskräften in der Wirtschaft sehen dies 35 Prozent so. Einkommensverlust

gilt 11 Prozent der Abgeordneten, jedoch nur 4 Prozent der Führungskräfte aus der Wirtschaft als künftig stark steigendes Risiko. Bei den IT- und Datenrisiken gehen die Einschätzungen im Ganzen dagegen kaum auseinander. Die Abgeordneten stufen Datenmissbrauch als künftiges Risiko etwas höher ein (Abgeordnete: 37 Prozent; Führungskräfte aus der Wirtschaft: 29 Prozent). Die Führungskräfte aus der Wirtschaft sehen stärker als Abgeordnete im Datenbetrug im Internet ein steigendes Risikopotenzial für die Zukunft (Abgeordnete: 5 Prozent; Führungskräfte aus der Wirtschaft: 10 Prozent, Tabelle 1).

Tabelle 1

Bewertung künftiger Risikopotenziale – differenziert nach Politikern und Führungskräften in Unternehmen

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

Diese Risiken werden in Zukunft besonders stark zunehmen –	Entscheider aus –	
	Politik %	Wirtschaft %
Altersrisiken (Altersarmut, Pflegebedürftigkeit, Demenz)	52	35
Datenmissbrauch	37	29
Internet-, Computerkriminalität, IT-Sicherheit, Internetrisiken	21	20
Naturkatastrophen, Umweltkrisen	18	17
Einkommensverlust	11	4
Verunreinigte, belastete Nahrungsmittel	9	6
Dass der Staat die Bürger zu sehr überwacht	7	7
Terroranschläge	6	4
Datenbetrug im Internet	5	10
Arbeitslosigkeit	5	4
Ökonomische Risiken, z.B. Finanz- und Wirtschaftskrisen	3	5
Inflation	1	6
Diebstahl, Einbruch und ähnliche Verbrechen	1	5

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

Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

BIG DATA – ENTSCHEIDER SEHEN EHER RISIKEN ALS NUTZEN FÜR DIE VERBRAUCHER

Die Aggregation und intelligente Analyse von großen Mengen an Kundendaten bieten aus Sicht vieler Branchenexperten unter dem Schlagwort „Big Data“ große Chancen für Unternehmen, ihre Wertschöpfungskette – von der Produktentwicklung bis zu Marketing und Vertrieb – zu optimieren. Die Bevölkerung betrachtet die Speicherung und Auswertung von Kundendaten allerdings grundsätzlich skeptisch. Besonders bei der gezielten Analyse von Verbraucherdaten für Marketingzwecke sowie für die Prüfung der individuellen Kreditwürdigkeit nimmt die Mehrheit der Bürger eine ablehnende Haltung ein.²

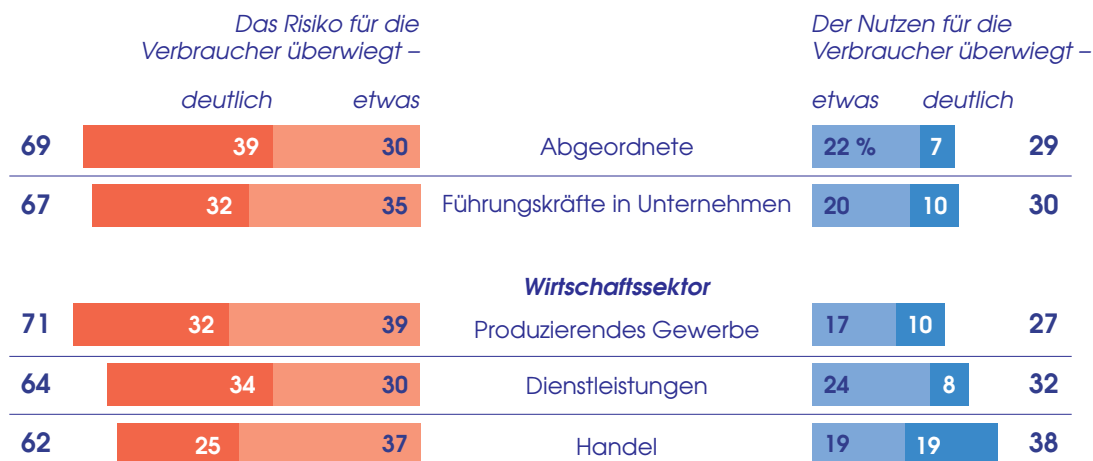
Die Entscheider aus Politik und Wirtschaft teilen diese skeptische Haltung. Aus Sicht der überwiegenden Mehrheit sowohl der Abgeordneten als auch der Führungskräfte in der Wirt-

schaft überwiegen bei der Speicherung von Kundendaten und Analyse von Big Data für die Verbraucher eher die Risiken im Vergleich zum Nutzen. Unter den Abgeordneten sind lediglich 29 Prozent der Auffassung, dass der Nutzen deutlich oder etwas überwiegt. 69 Prozent vertreten die Meinung, dass das Risiko deutlich oder etwas überwiegt. Bei den Führungskräften aus der Wirtschaft präsentiert sich das Bild nahezu identisch: 30 Prozent gehen davon aus, dass der Nutzen überwiegt; 67 Prozent sehen dagegen mehr Risiken als Nutzen. Lediglich Führungskräfte aus dem Handel sehen die Sammlung und Auswertung von Kundendaten in einem etwas besseren Licht. Aber auch unter ihnen überwiegt mit 62 Prozent zu 38 Prozent die Auffassung, dass Big Data eher Nachteile als Nutzen für die Verbraucher mit sich bringt (Schaubild 5).

Schaubild 5

Big Data bietet aus Sicht der Entscheider aus Politik und Wirtschaft mehr Risiken als Nutzen für die Verbraucher

Frage: „Wenn es um die Sammlung und Auswertung von Kundendaten durch Unternehmen geht, was überwiegt da aus Ihrer Sicht für die Verbraucher: der Nutzen, z. B. dass man von den Unternehmen individuelle Angebote erhält, oder das Risiko, dass die eigenen Daten missbraucht werden?“



Auf 100 fehlende Prozent: unentschieden, keine Angabe

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

Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

²Vgl. Deutsche Telekom/T-Systems, Sicherheitsreport 2013, S. 13 ff.

BIG DATA – ENTSCHEIDER SEHEN EHER RISIKEN ALS NUTZEN FÜR DIE VERBRAUCHER

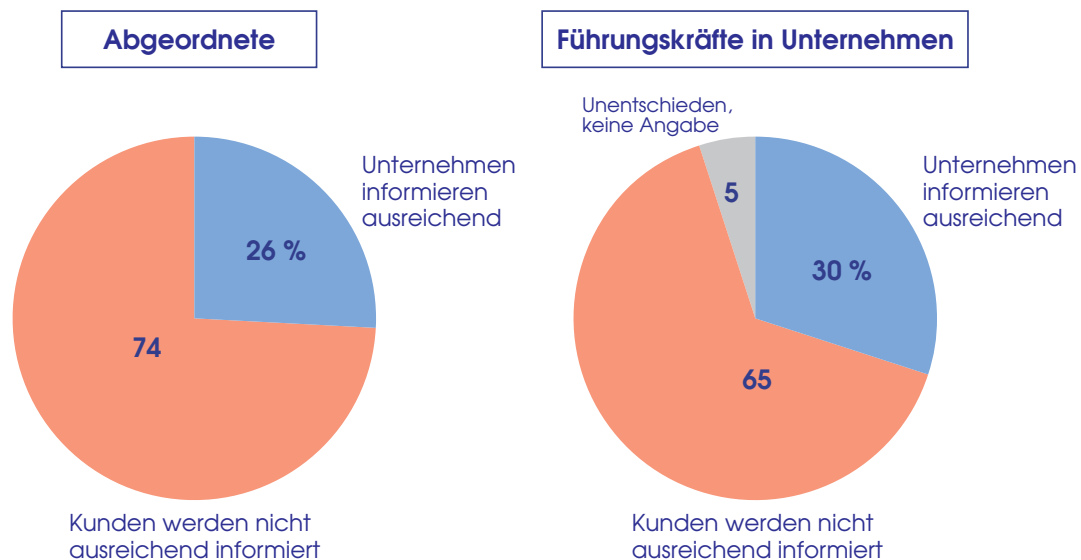
Ebenfalls kritisch zeigen sich die Entscheider im Hinblick auf die derzeitige Praxis der Speicherung und Auswertung von Kundendaten: 74 Prozent der Abgeordneten und 65 Prozent der Führungskräfte aus Unternehmen haben den Eindruck, dass Unternehmen ihre Kunden in der Regel nicht ausreichend

informieren, ob Kundendaten gespeichert bzw. wozu sie verwendet werden. Nur eine Minderheit von 26 Prozent der Politiker und 30 Prozent der Führungskräfte aus der Wirtschaft sieht eine ausreichende Informationspolitik der Unternehmen gegenüber ihren Kunden (Schaubild 6).

Schaubild 6

Keine ausreichende Information der Verbraucher über Speicherung und Verwendung ihrer Daten

Frage: „Haben Sie generell den Eindruck, dass Unternehmen ihre Kunden in der Regel ausreichend darüber informieren, ob sie deren Daten speichern bzw. wozu sie die Daten verwenden, oder werden die Kunden darüber nicht ausreichend informiert?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

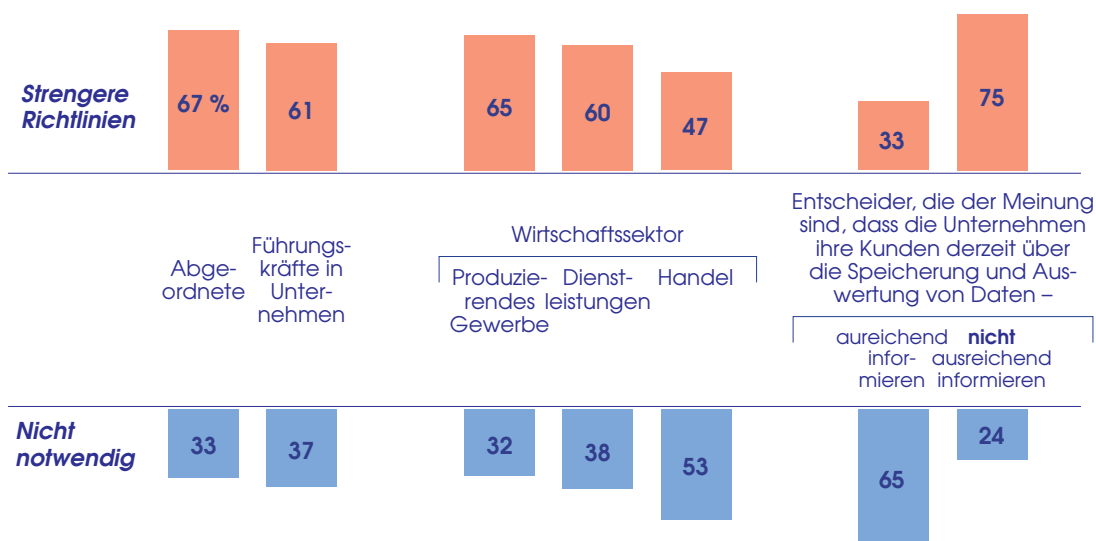
Dementsprechend verwundert es nicht, dass die Mehrheit der Entscheider strengere Richtlinien in diesem Bereich fordert. 67 Prozent der Abgeordneten und 61 Prozent der Führungskräfte aus der Wirtschaft vertreten die Ansicht, dass es bei der Speicherung und Verwendung von Kundendaten strengere Richtlinien geben sollte. Besonders deutlich fällt das Meinungsbild unter denjenigen Entscheidern aus, die der Meinung

sind, dass Unternehmen derzeit nicht ausreichend über die Speicherung und Verwendung von Kundendaten informieren. Von ihnen sind 75 Prozent der Auffassung, dass es strengerer Richtlinien bedürfe. Im Branchenvergleich halten lediglich Führungskräfte aus dem Handel strengere Richtlinien für nicht erforderlich (Schaubild 7).

Schaubild 7

Strengere Richtlinien für die Speicherung und Verwendung von Kundendaten

Frage: „Müsste es Ihrer Meinung nach in diesem Bereich, also bei der Speicherung und Verwendung von Kundendaten, strengere Richtlinien geben, welche Daten gespeichert und wie sie verwendet werden dürfen, oder halten Sie das nicht für notwendig?“



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

BIG DATA – ENTSCHEIDER SEHEN EHER RISIKEN ALS NUTZEN FÜR DIE VERBRAUCHER

Diejenigen, die sich strengere Richtlinien für die Speicherung und Auswertung von Kundendaten wünschen, halten hierzu gesetzliche Vorgaben für effektiver als eine stärkere Selbstverpflichtung der Unternehmen. So geben 71 Prozent der Abgeordneten und 53 Prozent der Führungskräfte in Unternehmen,

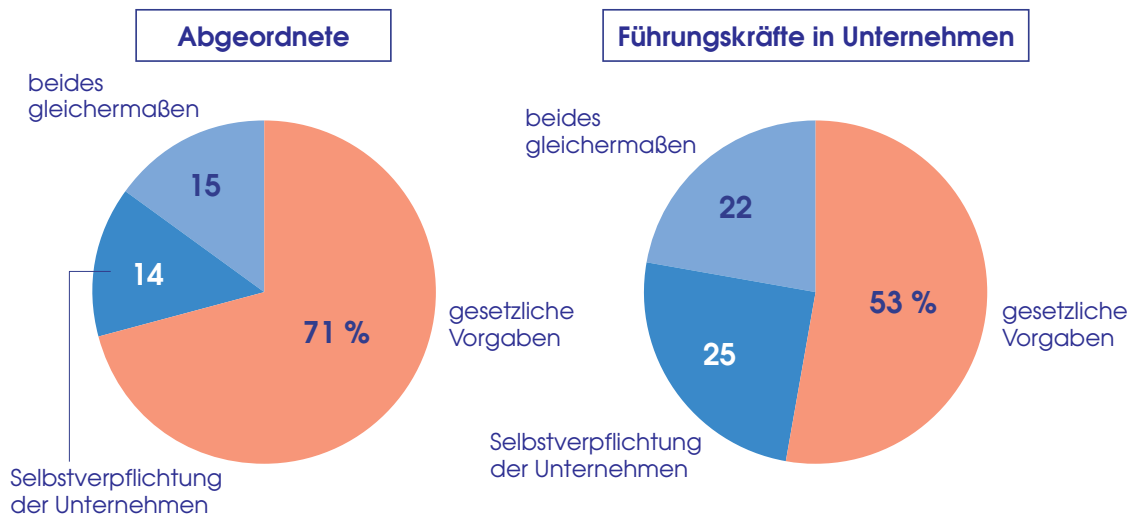
die sich für strengere Richtlinien aussprechen, gesetzlichen Vorrang den Vorzug. Nur 14 Prozent der Abgeordneten und 25 Prozent der Führungskräfte, die strengere Richtlinien für erforderlich halten, präferieren dazu eine stärkere Selbstverpflichtung der Unternehmen (Schaubild 8).

Schaubild 8

Strengere Richtlinien eher über gesetzliche Vorgaben als über Selbstverpflichtung der Unternehmen

Frage: „Wie sollte das geschehen: durch gesetzliche Vorgaben des Staates oder durch eine stärkere Selbstverpflichtung der Unternehmen?“

Von denjenigen, die strengere Richtlinien für erforderlich halten, plädieren für –



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen, die strengere Richtlinien im Bereich Kundendatenspeicherung/-verwendung für erforderlich halten
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

HOHER STELLENWERT DER IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

Die IT-Sicherheit hat heute für praktisch alle mittleren und großen Unternehmen einen hohen Stellenwert. 92 Prozent der Unternehmen messen dem Schutz des eigenen IT-Netzwerks vor unerlaubten Zugriffen von außen einen hohen oder sehr hohen Stellenwert bei. Dabei steigt die Bedeutung der IT-Sicherheit mit der Unternehmensgröße deutlich an, insbesondere nimmt der Anteil der Unternehmen, die der IT-Sicherheit

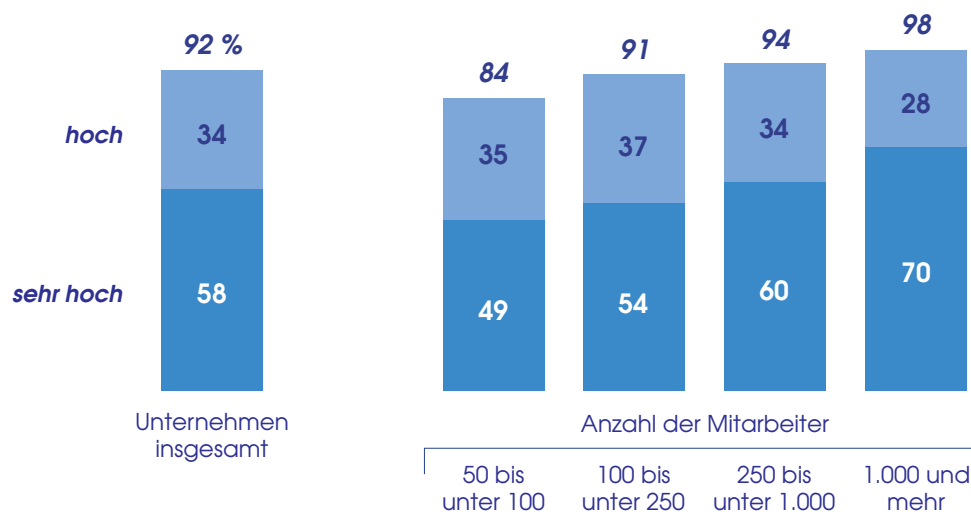
eine sehr hohe Bedeutung beimessen, stark zu. So geben von den Unternehmen mit 50 bis 100 Mitarbeitern 49 Prozent einen sehr hohen, 35 Prozent einen hohen Stellenwert der IT-Sicherheit zu Protokoll. Von den Unternehmen mit 1.000 und mehr Mitarbeitern messen 70 Prozent der IT-Sicherheit einen sehr hohen, 28 Prozent einen hohen Stellenwert bei (Schaubild 9).

Schaubild 9

Stellenwert der IT-Sicherheit nimmt mit der Unternehmensgröße zu

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 –



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

HOHER STELLENWERT VON IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

Der hohe Stellenwert der IT-Sicherheit in mittleren und großen Unternehmen geht auch mit höheren Kosten einher. 35 Prozent der Unternehmen berichten über deutlich, 41 Prozent über etwas gestiegene Kosten für die IT-Sicherheit. Lediglich in 14 Prozent der Fälle sind die Kosten für den Schutz vor Hackerangriffen in den letzten Jahren nicht gestiegen. Dabei ist für das Ausmaß der Kostenzunahme weniger die Unternehmensgröße entscheidend als vielmehr die Frage, welchen Stellenwert der IT-Sicherheit im Unternehmen beigemessen

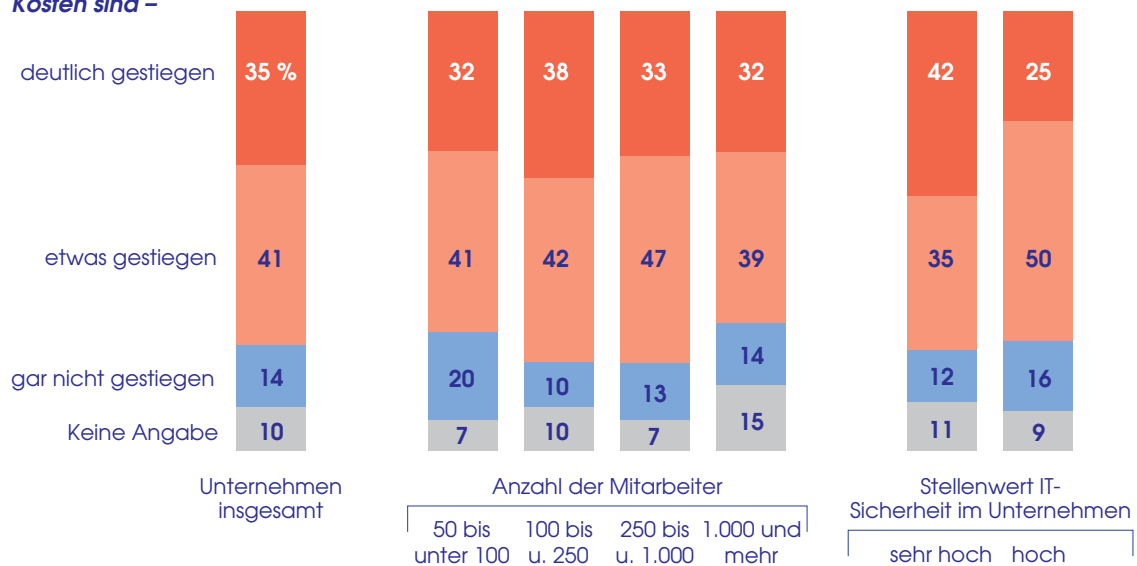
wird. So schwankt der Anteil der Unternehmen, die einen deutlichen Kostenanstieg verzeichneten, in Abhängigkeit von der Unternehmensgröße lediglich zwischen 32 und 38 Prozent. Von Unternehmen, die der IT-Sicherheit einen sehr hohen Stellenwert einräumen, berichten dagegen 42 Prozent über einen deutlichen Kostenanstieg. In Unternehmen, in denen die IT-Sicherheit „nur“ einen hohen Stellenwert hat, sind es 25 Prozent (Schaubild 10).

Schaubild 10

Steigende Kosten für IT-Sicherheit

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

Kosten sind –



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Die ganz überwiegende Zahl der mittleren und großen Unternehmen in Deutschland berichtet über IT-Angriffe von außen. Nur 13 Prozent der Unternehmen, die eine konkrete Angabe zur Häufigkeit von IT-Angriffen gemacht haben, berichten über keine Angriffe.³ 20 Prozent der Unternehmen werden mehr-

mals in der Woche oder sogar täglich attackiert (12 Prozent täglich, 8 Prozent mehrmals in der Woche), 24 Prozent zwischen einmal im Monat und einmal in der Woche (5 Prozent etwa einmal in der Woche, 10 Prozent 2- bis 3-mal im Monat, 9 Prozent etwa einmal im Monat). 43 Prozent der Unterneh-

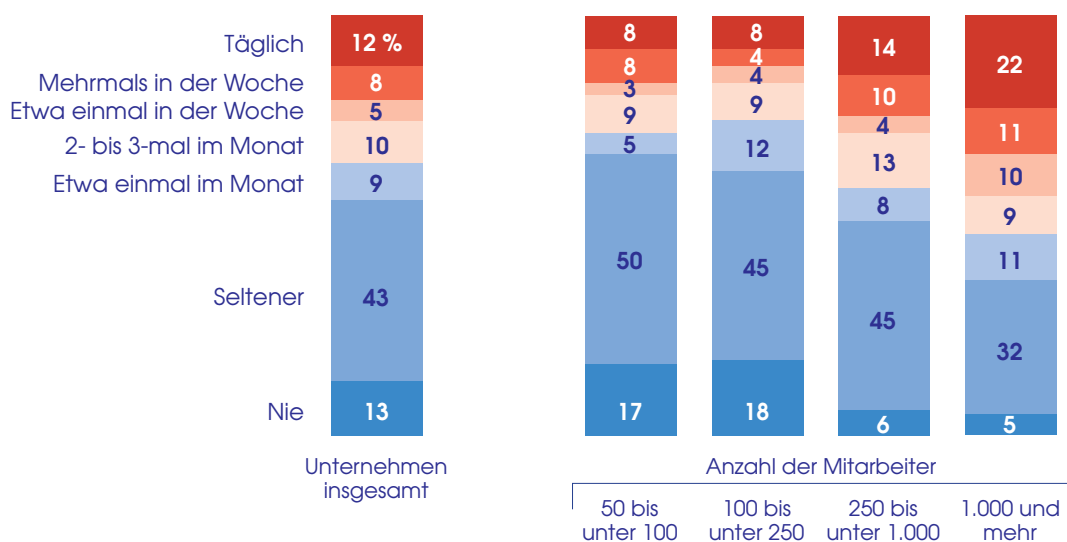
men registrieren seltener Angriffe auf ihr IT-Netzwerk⁴. Die Häufigkeit der Angriffe hängt stark von der Größe des Unternehmens ab. So verzeichnen von den Unternehmen, die zwischen 50 und 100 Mitarbeiter haben, 16 Prozent täglich

oder mehrmals in der Woche Angriffe, von den Unternehmen mit 1.000 und mehr Mitarbeitern sind es 33 Prozent (Schaubild 11).

Schaubild 11

Deutsche Unternehmen als Ziel von IT-Angriffen

Frage: „Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt, durch die Ihr Unternehmen aus-
gespioniert 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 6267 (Juni/Juli 2013)

© IfD-Allensbach

³ 22 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: 10 Prozent; mehrmals in der Woche: 6 Prozent; etwa einmal in der Woche: 4 Prozent; 2- bis 3-mal im Monat: 7 Prozent; etwa einmal im Monat: 7 Prozent; seltener: 34 Prozent; nie: 10 Prozent; Unmöglich zu sagen, keine Angabe: 22 Prozent.

⁴ Soweit im Folgenden die Unternehmen bei der Häufigkeit der IT-Angriffe nach „häufig“, „gelegentlich“ und „selten/nie“ unterschieden werden, werden unter „häufig“ alle Unternehmen subsumiert, die täglich oder mehrmals in der Woche IT-Angriffen ausgesetzt sind. Unter „gelegentlich“ werden Unternehmen eingeordnet, die zwischen einmal in der Woche und einmal im Monat Angriffe registrieren. Unternehmen, die seltener oder nie attackiert werden, sind unter der Bezeichnung „selten/nie“ zusammengefasst.

HOHER STELLENWERT VON IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

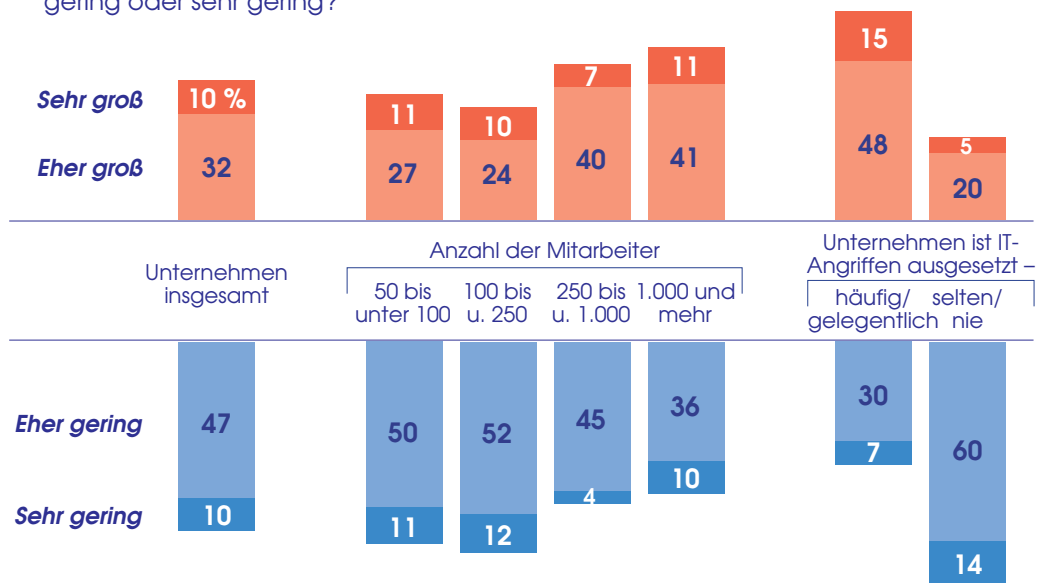
Die Mehrheit der Führungskräfte in mittleren und großen Unternehmen stuft das Risiko, durch einen Hackerangriff gravierend geschädigt zu werden, als eher oder sehr gering ein. 10 Prozent sehen darin ein sehr geringes Risiko, 47 Prozent ein eher geringes Risiko. Ein sehr großes Risiko sehen darin dagegen 10 Prozent, ein eher großes Risiko 32 Prozent. Mit der Unternehmensgröße nimmt diese Gefahreinschätzung deutlich zu. Von den Unternehmen mit weniger als 250 Mitarbeitern stuft nur 38 bzw. 34 Prozent das Risiko als sehr groß oder groß ein; von den Unternehmen mit 1.000 und

mehr Mitarbeitern ist es mit 52 Prozent dagegen die Mehrheit. Die Risikoeinschätzung hängt auch erheblich davon ab, wie häufig das Unternehmen IT-Angriffen ausgesetzt ist. Von den Unternehmen, die über häufige oder gelegentliche IT-Angriffe berichten, stuft 63 Prozent das Risiko gravierender Schäden durch solche Angriffe als groß ein. Von den Unternehmen, die selten oder nie Ziel externer Angriffe sind, sind es weniger als halb so viele, nämlich 25 Prozent, die von einem gravierenden Schadensrisiko durch Hackerangriffe ausgehen (Schaubild 12).

Schaubild 12

Mehrheit der Unternehmen stuft das Schadensrisiko durch einen Hackerangriff als (eher) gering 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 6267 (Juni/Juli 2013)

© IfD-Allensbach

Im Vergleich zum Vorjahr ist das Risikobewusstsein dabei in der vergleichbaren Gruppe von großen Unternehmen gestiegen. Vor einem Jahr stuften 42 Prozent der Führungskräfte in großen Unternehmen das Risiko, dass ihr Unternehmen

durch einen Hackerangriff gravierend geschädigt würde, als sehr groß oder eher groß ein; aktuell sind es 53 Prozent. Im Gegenzug sank der Anteil, der ein geringes Risiko durch einen solchen Angriff vermutet, von 56 auf 45 Prozent (Tabelle 2).

Tabelle 2

Gestiegenes Risikobewusstsein				
Es halten das Risiko, dass ihr Unternehmen durch einen Hackerangriff gravierend geschädigt wird, für –	2012 %		2013 %	
sehr groß	10	} 42	10	} 53
eher groß	32		43	
eher gering	48	} 56	39	} 45
sehr gering	8		6	

Auf 100 fehlende Prozent: keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in großen Unternehmen, Quelle: Allensbacher Archiv, IfD-Umfragen 6240 und 6267 (Juni/Juli 2013)

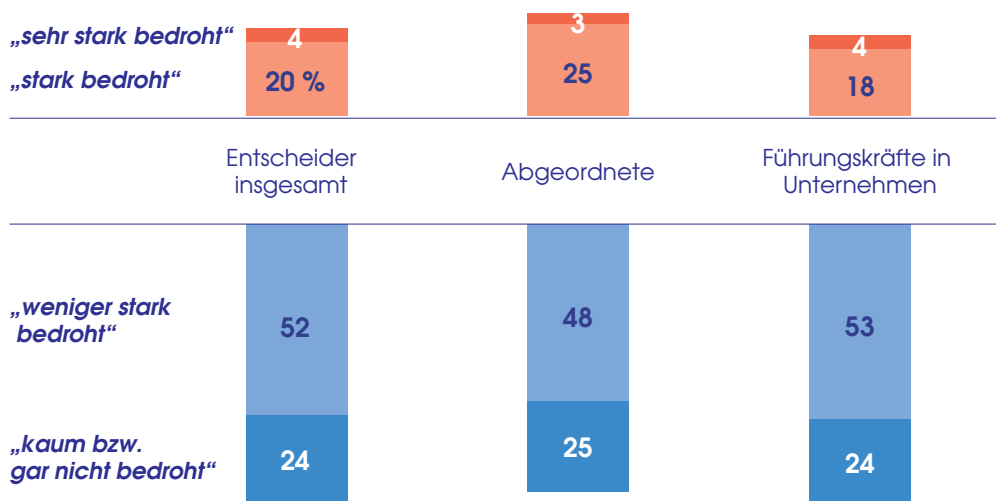
Persönlich durch IT-Angriffe bedroht fühlt sich übrigens nur eine Minderheit der Entscheider aus Politik und Wirtschaft. 24 Prozent fühlen sich sehr stark oder stark dadurch bedroht, dass ihr Smartphone oder Computer gehackt werden oder dass sich jemand mit ihren Passwörtern Zugang zu persönlichen oder unternehmensinternen Daten verschaffen könnte. 76 Pro-

zent fühlen sich hingegen weniger stark oder kaum bzw. gar nicht bedroht. Abgeordnete schätzen das Bedrohungspotenzial dabei etwas größer ein als Führungskräfte in der Wirtschaft: Von den Abgeordneten fühlen sich 28 Prozent sehr stark oder stark bedroht, von den Führungskräften in mittleren und großen Unternehmen sind es 22 Prozent (Schaubild 13).

Schaubild 13

Exkurs: persönliche Bedrohung durch IT-Angriffe

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 verschaffen könnte? 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-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

HOHER STELLENWERT VON IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

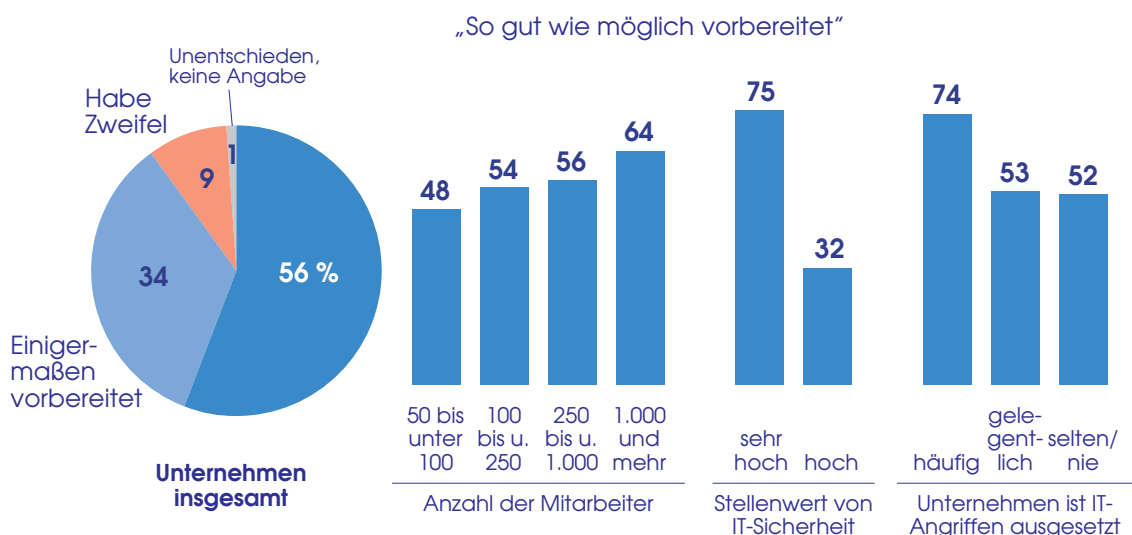
Die Mehrheit der Führungskräfte aus mittleren und großen Unternehmen sieht ihr Unternehmen gut auf mögliche Gefahren für die IT-Sicherheit vorbereitet. 56 Prozent haben das Gefühl, dass ihr Unternehmen so gut wie möglich vorbereitet ist, 34 Prozent sehen es zumindest einigermaßen gerüstet. Lediglich 9 Prozent äußern Zweifel, dass ihr Unternehmen gut oder zumindest einigermaßen 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 Unter-

nehmen mit 50 bis 100 Mitarbeitern zeigt sich rund die Hälfte überzeugt, bestmöglich gegen potenzielle Gefahren für die IT-Sicherheit gewappnet zu sein; von den Unternehmen mit 1.000 und mehr Mitarbeitern sind es 64 Prozent. Besonders gut fühlen sich Unternehmen vorbereitet, für die die IT-Sicherheit im Unternehmen einen sehr hohen Stellenwert hat. Von ihnen sehen sich 75 Prozent sehr gut für mögliche Gefahren für die IT-Sicherheit gerüstet. Und auch Unternehmen, die häufig IT-Angriffen ausgesetzt sind, fühlen sich mit 74 Prozent weit überdurchschnittlich gut auf mögliche IT-Gefahren vorbereitet (Schaubild 14).

Schaubild 14

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 6267 (Juni/Juli 2013)

© IfD-Allensbach

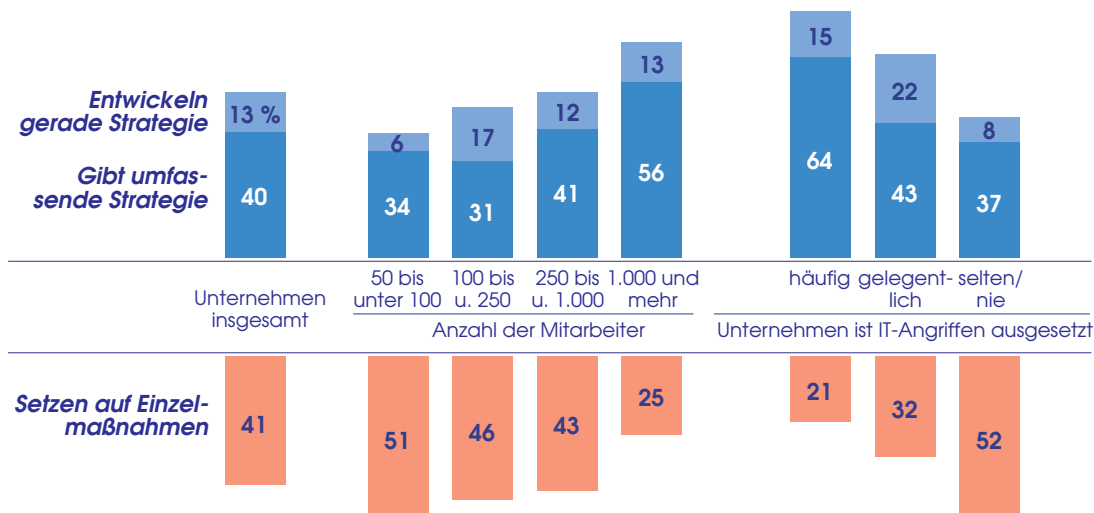
Die Mehrheit der Unternehmen besitzt nach eigenem Bekunden eine umfassende Strategie zum Umgang mit Cybergefahren bzw. baut gegenwärtig eine solche Strategie auf. 40 Prozent der mittleren und großen Unternehmen haben bereits eine umfassende Strategie, wie sie mit Cybergefahren umgehen; 13 Prozent sind derzeit dabei, eine solche Strategie zu entwickeln. 41 Prozent setzen indes weniger auf eine umfassende Strategie, sondern vielmehr auf verschiedene Einzelmaßnahmen. Je größer das Unternehmen, desto eher setzt es auf eine umfassende Strategie statt auf Einzelmaßnahmen. So hat von den Unternehmen mit 50 bis 100 Mitarbeitern rund jedes dritte eine umfassende Strategie, wie Cybergefahren begegnet wird.

Von Unternehmen mit 1.000 Mitarbeitern und mehr ist es mehr als jedes zweite. Einen großen Einfluss auf die Existenz einer „Cyber-Security-Strategie“ hat zudem die Häufigkeit, mit der Unternehmen IT-Angriffen ausgesetzt sind. Je häufiger Unternehmen IT-Angriffe auf ihr Netzwerk registrieren, desto eher investieren sie offenbar auch in die Entwicklung einer umfassenden Strategie zum Schutz vor solchen Angriffen. Von den Unternehmen, die vermehrt das Ziel von IT-Angriffen sind, haben bereits 64 Prozent eine umfassende Strategie. Von den Unternehmen, die selten oder nie IT-Angriffe verzeichnen, sind es nur 37 Prozent (Schaubild 15).

Schaubild 15

Umfassende Strategie gegen Cybergefahren?

Frage: „Gibt es bei Ihnen im Unternehmen eine umfassende Strategie, wie Sie mit Cybergefahren umgehen, also mit Risiken, die sich durch das Internet und andere Datenetze ergeben, oder sind Sie gerade dabei, eine solche umfassende Strategie zu entwickeln und aufzubauen, oder setzen Sie zur Vermeidung von Cyberrisiken weniger auf eine umfassende Strategie als vielmehr auf verschiedene Einzelmaßnahmen?“



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

HOHER STELLENWERT VON IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

Unternehmen mit einer umfassenden Cyber-Security-Strategie sehen sich deutlich besser als andere Unternehmen auf mögliche Gefahren für die IT-Sicherheit vorbereitet. So sind 79 Prozent der Führungskräfte aus Unternehmen, die eine umfassende Strategie gegen IT-Angriffe haben, davon überzeugt, bestmöglich gegen Gefahren für die IT-Sicherheit gewappnet

zu sein. Von den Unternehmen, die aktuell erst eine solche Cyber-Security-Strategie aufbauen oder grundsätzlich auf Einzelmaßnahmen setzen, sind dies mit 39 Prozent nur etwa halb so viele. Aber auch in diesen Unternehmen fühlt man sich mehrheitlich zumindest einigermaßen auf IT-Gefahren vorbereitet (Tabelle 3).

Tabelle 3

Auf Gefahren besser vorbereitet mit Cyber-Security-Strategie			
Unternehmen ist auf mögliche Gefahren für die IT-Sicherheit vorbereitet –	Gegen Cyber-Risiken –		
	gibt es eine umfassende Strategie %	wird Strategie entwickelt %	setzt man auf Einzelmaßnahmen %
so gut wie möglich	79	39	39
einigermaßen	21	49	45
habe Zweifel	x	12	15
Unentschieden, keine Angabe	x	x	1

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

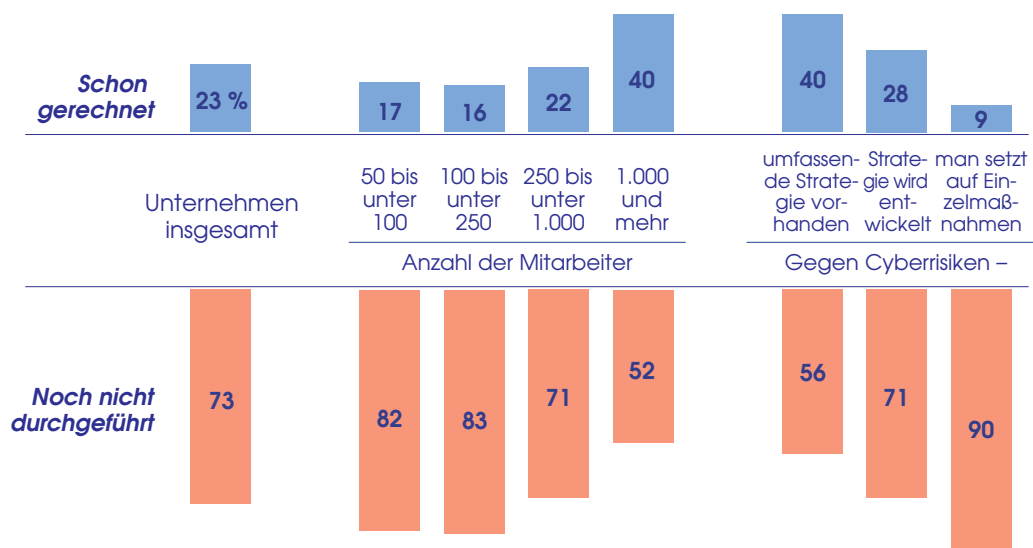
Obwohl sich viele Unternehmen gut bzw. zumindest einigermaßen auf IT-Angriffe vorbereitet fühlen und auch von einer umfassenden Strategie für den Umgang mit Cybergefahren berichten, hat nur eine Minderheit ein adäquates Risikomanagement etabliert. 23 Prozent der mittleren und großen Unternehmen insgesamt haben bereits konkret durchgerechnet, welche Kosten im Fall eines erfolgreichen IT-Angriffs auf ihr Unternehmen zukämen. 73 Prozent haben hingegen noch

keine entsprechenden Analysen durchgeführt, sich also nicht damit befasst, wie wahrscheinlich ein solches Szenario ist und welcher Schaden dabei entstünde. Am ehesten noch verfügen sehr große Unternehmen mit 1.000 und mehr Mitarbeitern über ein Risikomanagement für den Fall von IT-Angriffen. Von ihnen haben 40 Prozent die finanziellen Folgen eines IT-Angriffs beziffert (Schaubild 16).

Schaubild 16

Kaum Risikomanagement für den Fall von IT-Angriffen

Frage: „Haben Sie schon einmal konkret durchgerechnet, welche Kosten im Fall eines IT-Angriffs auf Ihr Unternehmen zukämen, also konkrete Analysen durchgeführt, wie wahrscheinlich ein solches Szenario ist und welcher Schaden dabei entstünde, oder haben Sie das noch nicht getan?“



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
 Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

HOHER STELLENWERT VON IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

Deutlich häufiger verfügen die Unternehmen über einen Notfallplan für Cyberangriffe. In fast jedem zweiten Unternehmen ist ein solcher Notfallplan vorhanden. Erneut zeigen sich große Unternehmen besser vorbereitet als mittlere Unternehmen. Von den Unternehmen mit 50 bis 100 Mitarbeitern haben 40 Prozent einen Notfallplan, von den Unternehmen mit 1.000 und mehr Mitarbeitern 63 Prozent. Und auch die Häufigkeit der IT-Angriffe spielt eine wichtige Rolle. 79 Prozent der Unternehmen, die häufig IT-Angriffen ausgesetzt sind, verfügen über ein Notfallkonzept. Von den Unternehmen, die gelegentlich Ziel von Hackerangriffen sind, sind es 53 Prozent. Von den Unternehmen, die nur selten oder nie Angriffe auf ihr Netzwerk

registrieren, haben 42 Prozent einen Notfallplan entwickelt. Ein Notfallplan gehört offensichtlich für die meisten Unternehmen auch zu einer umfassenden Strategie dazu. Denn 73 Prozent der Unternehmen, in denen eine umfassende Strategie zum Umgang mit Cyberrisiken vorhanden ist, haben auch einen Notfallplan.

Von den Unternehmen, in denen eine solche Cyber-Security-Strategie erst aufgebaut wird, hat rund jedes zweite einen Notfallplan. Unternehmen, die lediglich auf Einzelmaßnahmen zur Reaktion auf mögliche IT-Angriffe setzen, haben nur 29 Prozent einen Notfallplan in der Schublade liegen (Schaubild 17).

Schaubild 17

Notfallplan für Cyberangriffe vorhanden?

Frage: „Gibt es in Ihrem Unternehmen einen Notfallplan für Cyberangriffe, 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 6267 (Juni/Juli 2013)

© IfD-Allensbach

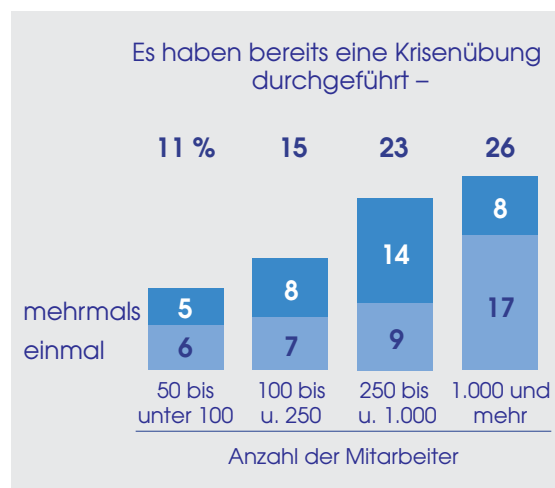
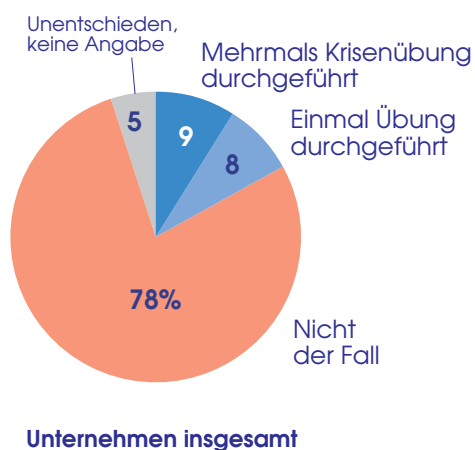
Die Simulation einer Krisensituation ist dagegen noch weitgehend Neuland für Unternehmen. Nur eine kleine Minderheit der Unternehmen hat bislang durchgespielt, wie man sich im Fall eines ernsthaften IT-Angriffs verhalten würde. 8 Prozent haben bereits einmal, 9 Prozent mehrmals einen Cyberangriff simuliert. 78 Prozent haben dies noch nie durchexerziert. Und auch hier

zeigen sich große Unternehmen besser vorbereitet als mittlere Unternehmen: Von den Unternehmen mit 50 bis 100 Mitarbeitern hat erst jedes zehnte eine Krisenübung durchgeführt, von den Unternehmen mit 1.000 und mehr Mitarbeitern immerhin schon jedes vierte (Schaubild 18).

Schaubild 18

Nur eine Minderheit der Unternehmen hat bereits eine Krisenübung durchgeführt

Frage: „Haben Sie im Unternehmen schon einmal oder schon mehrmals eine Krisenübung durchgeführt, also einen Cyberangriff simuliert, oder ist das nicht der Fall?“



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
 Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

HOHER STELLENWERT VON IT-SICHERHEIT IN DEN UNTERNEHMEN – ABER TEILWEISE DEUTLICHE UNTERSCHIEDE IN DER OPERATIVEN UMSETZUNG VON MASSNAHMEN

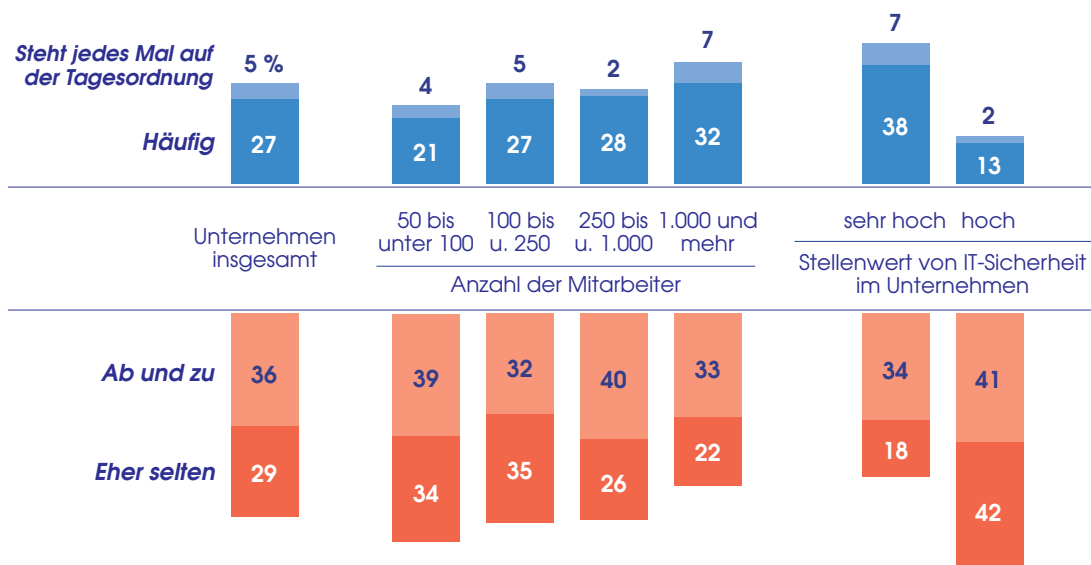
Die Relevanz des Themas IT-Sicherheit für das Topmanagement lässt sich nicht zuletzt auch daran ablesen, wie häufig es in Sitzungen des Vorstands oder der Geschäftsführung behandelt wird. Aktuell steht das Thema bei 5 Prozent der Unternehmen in jeder Sitzung des Vorstands bzw. der Geschäftsführung auf der Tagesordnung, bei 27 Prozent zumindest häufig. In der Mehrheit der Unternehmen findet sich IT-Sicherheit allerdings nur „ab und zu“ oder „eher selten“ auf der Sitzungsagenda wieder. Dabei hat zwar auch die Größe des Unternehmens einen Einfluss darauf, wie häufig IT-Sicherheit Thema in Vor-

stands- und Geschäftsführungsrunden ist. Ausschlaggebender ist aber vielmehr, welcher Stellenwert der IT-Sicherheit im Unternehmen beigemessen wird. In 45 Prozent der mittleren und großen Unternehmen, in denen die IT-Sicherheit einen sehr hohen Stellenwert einnimmt, steht das Thema häufig oder sogar jedes Mal auf der Tagesordnung des Topmanagements. Von den Unternehmen, die der IT-Sicherheit „nur“ einen hohen Stellenwert beimessen, haben das Thema indes lediglich 15 Prozent derart regelmäßig auf der Sitzungsagenda von Vorstand bzw. Geschäftsführung stehen (Schaubild 19).

Schaubild 19

IT-Sicherheit ist eher sporadisch Thema bei Sitzungen des Vorstandes bzw. der Geschäftsführung

Frage: „Wie ist das bei Ihnen im Unternehmen: Wie häufig steht das Thema IT-Sicherheit bei Sitzungen des Vorstands bzw. der Geschäftsführung auf der Tagesordnung?“



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Somit steht die IT-Sicherheit zwar nur sporadisch auf der Tagesordnung von Vorstands- und Geschäftsführungssitzungen. Die Führungskräfte sehen allerdings auch kaum Bedarf an einer häufigeren Diskussion von IT-Sicherheitsthemen in diesem Kreis. 84 Prozent der Führungskräfte, in deren Unternehmen die IT-Sicherheit nicht bereits bei jeder Sitzung von Vorstand bzw. Geschäftsführung Bestandteil der Tagesordnung ist, halten

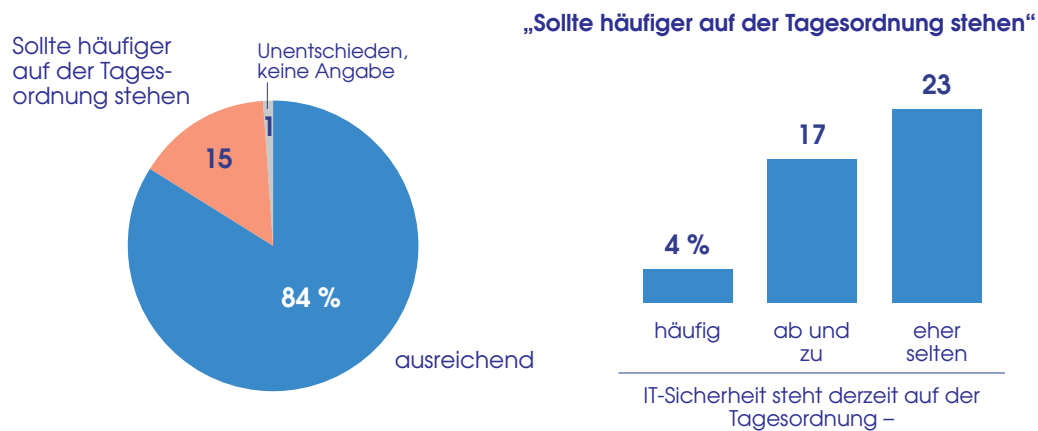
die derzeitige Frequenz für ausreichend; nur 15 Prozent sind der Meinung, das Thema sollte häufiger auf die Agenda gesetzt werden. Selbst in Unternehmen, in denen die IT-Sicherheit derzeit eher selten auf der Tagesordnung steht, halten nur 23 Prozent der Führungskräfte eine häufigere Behandlung des Themas in Sitzungen des Topmanagements für erforderlich (Schaubild 20).

Schaubild 20

Führungskräfte sehen kaum Bedarf an häufiger Diskussion von IT-Sicherheitsthemen in Sitzungen des Vorstands bzw. der Geschäftsführung

Frage: „Finden Sie das ausreichend, oder müsste das Thema IT-Sicherheit eigentlich (noch) häufiger bei Sitzungen des Vorstands bzw. der Geschäftsführung auf der Tagesordnung stehen?“

Von den Führungskräften, in deren Unternehmen die IT-Sicherheit nicht bei jeder Sitzung von Vorstand bzw. Geschäftsführung auf der Tagesordnung steht, halten die derzeitige Frequenz für –



Basis: Bundesrepublik Deutschland; Führungskräfte in mittleren und großen Unternehmen, in deren Unternehmen das Thema IT-Sicherheit nicht bei jeder Sitzung von Vorstand bzw. Geschäftsführung auf der Tagesordnung steht
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

GEFAHRENQUELLEN UND HERAUSFORDERUNGEN IM BEREICH IT-SICHERHEIT – VERHALTEN DER MITARBEITER ALS GRÖSSTES RISIKO

Stellt man verschiedene potenzielle Gefahrenquellen für die IT-Sicherheit zur Abstimmung, so gelten aus Sicht der Führungskräfte in mittleren und großen Unternehmen vor allem Mitarbeiter, aber auch die Nutzung mobiler Endgeräte als sehr große oder große Gefahr. Hackerangriffe werden hingegen als eher nachrangige Gefahrenquellen eingestuft. 57 Prozent der Führungskräfte sehen in Mitarbeitern, die leichtfertig mit Daten umgehen oder Sicherheitsstandards nicht beachten, eine sehr große oder große Gefahr für die IT-Sicherheit im eigenen Unternehmen. Ähnlich groß wird mit 50 Prozent das Bedrohungspotenzial eingeschätzt, das von der Nutzung mobiler

Endgeräte wie Smartphones oder Tablet-PCs für die IT-Sicherheit ausgeht: 16 Prozent stufen dies als sehr große, 34 Prozent als große Gefahr ein. Mit deutlichem Abstand folgen andere potenzielle Gefahrenquellen. Der Datenmissbrauch, beispielsweise durch die unerlaubte Weitergabe von Daten durch Mitarbeiter, wird von 36 Prozent der Führungskräfte als sehr große oder große Gefahr betrachtet. Hackerangriffe beurteilen 31 Prozent der Führungskräfte als (sehr) große Gefahr. 26 Prozent sehen schließlich im Einsatz veralteter Technik eine sehr große oder große Bedrohung für das Unternehmen (Schaubild 21).

Schaubild 21

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?“

<i>Davon geht für die IT-Sicherheit im Unternehmen aus –</i>	<i>„eine sehr große Gefahr“</i>	<i>„eine große Gefahr“</i>	<i>Summe %</i>
Wenn Mitarbeiter leichtfertig mit Daten umgehen und Sicherheitsstandards nicht beachten	19 %	38	57
Durch die Nutzung mobiler Endgeräte wie Smartphones oder Tablet-PCs	16	34	50
Datenmissbrauch, z. B. durch unerlaubte Weitergabe von Daten durch Mitarbeiter des Unternehmens	6	30	36
Hacker-Angriffe auf das Unternehmen	6	25	31
Der Einsatz veralteter Technik	7	19	26

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Bei zwei der fünf Risiken gibt es einen deutlichen Zusammenhang zwischen der Einschätzung ihrer Bedeutung und der Unternehmensgröße. So stufen 48 Prozent der Führungskräfte aus Unternehmen mit 50 bis 100 Mitarbeitern die Gefahr für die IT-Sicherheit als sehr groß oder groß ein, welche auf die Sorglosigkeit von Beschäftigten zurückzuführen ist. Von den

Führungskräften aus Unternehmen mit 1.000 und mehr Mitarbeitern sind es 68 Prozent. Hackerangriffe werden von 28 Prozent der Führungskräfte in Unternehmen mit 50 bis 100 Beschäftigten als (sehr) großes Risiko angesehen. Von den Führungskräften in Unternehmen mit 1.000 und mehr Mitarbeitern sind es 44 Prozent (Tabelle 4).

Tabelle 4

Teilweise deutlicher Zusammenhang zwischen Unternehmensgröße und Risikobewertung

	Anzahl der Mitarbeiter			
	50 bis unter 100 %	100 bis u. 250 %	250 bis u. 1.000 %	1.000 und mehr %
Es stufen als sehr große oder große Gefahrenquelle für die IT-Sicherheit des Unternehmens ein –				
Wenn Mitarbeiter leichtfertig mit Daten umgehen und Sicherheitsstandards nicht beachten	48	54	60	68
Hackerangriffe auf das Unternehmen	28	26	29	44

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
 Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

GEFAHRENQUELLEN UND HERAUSFORDERUNGEN IM BEREICH IT-SICHERHEIT – VERHALTEN DER MITARBEITER ALS GRÖSSTES RISIKO

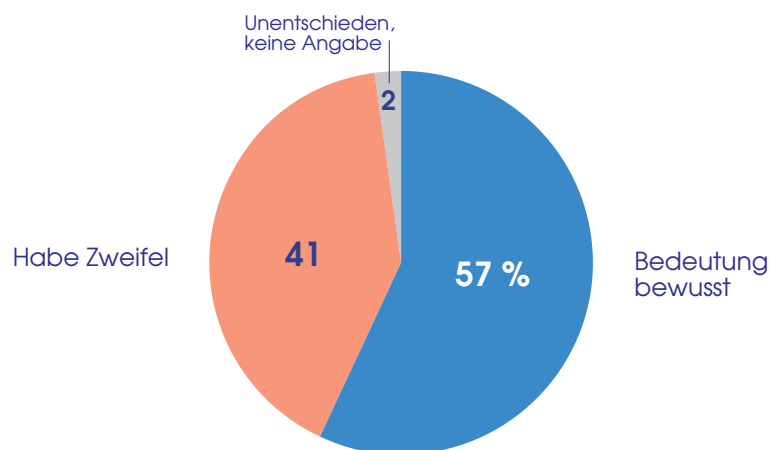
Die Mehrheit der Führungskräfte hat gleichwohl den Eindruck, dass den meisten Mitarbeitern die Bedeutung des Themas IT-Sicherheit bewusst ist. 57 Prozent vertreten die Meinung,

dass die meisten Beschäftigten bei ihnen im Unternehmen verantwortungsvoll mit Daten und möglichen IT-Risiken umgehen, 41 Prozent haben Zweifel (Schaubild 22).

Schaubild 22

Eindruck der Führungskräfte in den Unternehmen: Den meisten Mitarbeitern ist die Bedeutung des Themas IT-Sicherheit bewusst

Frage: „Haben Sie den Eindruck, dass sich die meisten Mitarbeiter bei Ihnen im Unternehmen der Bedeutung des Themas IT-Sicherheit ausreichend bewusst sind und verantwortungsvoll mit Daten und möglichen IT-Risiken umgehen, oder haben Sie da Zweifel?“



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Der leichtfertige Umgang der Mitarbeiter als größte potenzielle Gefahrenquelle für die IT-Sicherheit spiegelt sich auch im Handlungsbedarf bezüglich der IT-Sicherheit wider, den die Führungskräfte bei sich im Unternehmen sehen. Auf die offene Frage – also ohne Antwortvorgaben –, in welchen Bereichen sie in ihrem Unternehmen den größten Handlungsbedarf bezüglich der IT-Sicherheit sehen, nennen 23 Prozent der Führungskräfte die Schulung, Information und Sensibilisierung der Mitarbeiter. Von den Führungskräften, die für den IT-Bereich

ihres Unternehmens verantwortlich sind, betrachten sogar 31 Prozent die Schulung, Information und Sensibilisierung der Mitarbeiter als besonders wichtige Aufgabe im Kontext mit der IT-Sicherheit im Unternehmen. Erst mit deutlichem Abstand folgt der Schutz vor IT-Angriffen von außen, der von 12 Prozent der Führungskräfte spontan genannt wird. 8 Prozent betrachten eine funktionierende technische Schutzbarriere als besonders wichtiges Handlungsfeld für die IT-Sicherheit, genauso viele sehen in der Gewährleistung von Datensicherheit den

größten Handlungsbedarf. Ebenfalls 8 Prozent sehen eine große Herausforderung darin, immer auf dem aktuellsten Stand zu sein. Andere als vordringlich gesehene Aufgaben werden

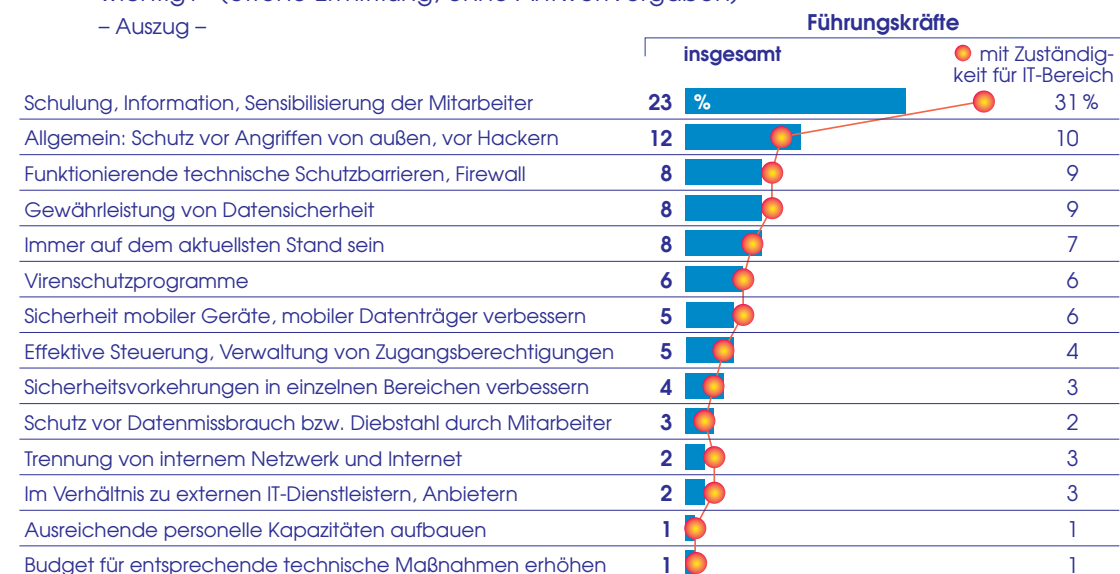
jeweils spontan nur von 6 Prozent oder weniger der Führungskräfte genannt (Schaubild 23).

Schaubild 23

Handlungsbedarf bei der IT-Sicherheit im eigenen Unternehmen

Frage: „Wenn Sie einmal an die IT-Sicherheit bei Ihnen im Unternehmen denken: Wo sehen Sie da ganz allgemein den größten Handlungsbedarf, was halten Sie für besonders wichtig?“ (offene Ermittlung, ohne Antwortvorgaben)

– Auszug –



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Das „Cloud Computing“ als Möglichkeit, eigene Daten und Programme extern im Internet statt auf dem eigenen Computer oder Firmenserver zu speichern, stößt bei den Entscheidern auf erhebliche Sicherheitsbedenken. Von den Führungskräften in den mittleren und großen Unternehmen halten diese Art der Datenverarbeitung nur 2 Prozent für sehr sicher, 21 Prozent für eher sicher. Die überwiegende Mehrheit hält das Cloud Computing dagegen für eher unsicher (46 Prozent) oder sehr unsicher (23 Prozent). Auch Führungskräfte, die in ihrem Un-

ternehmen für den IT-Bereich verantwortlich sind, sehen das Cloud Computing kritisch. Bei den Abgeordneten stößt das Cloud Computing ebenfalls auf Skepsis. 33 Prozent der Politiker sehen das Cloud Computing als sicher an, 61 Prozent dagegen als unsicher (Schaubild 24).

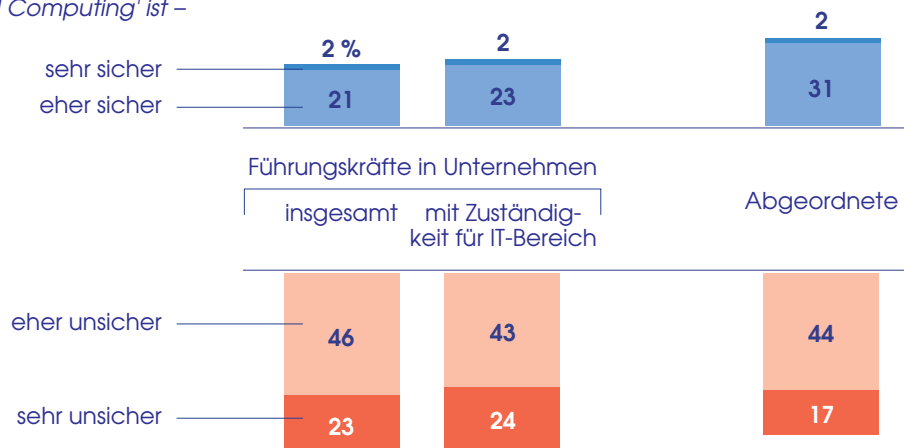
GEFAHRENQUELLEN UND HERAUSFORDERUNGEN IM BEREICH IT-SICHERHEIT – VERHALTEN DER MITARBEITER ALS GRÖSSTES RISIKO

Schaubild 24

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'?“

'Cloud Computing' ist –



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 6267 (Juni/Juli 2013)

© IfD-Allensbach

Im Vergleich zu den Vorjahren ist der Anteil derjenigen, die das Cloud Computing als sicher betrachten, allerdings erneut leicht angestiegen. Nimmt man den gleichen Personenkreis wie in den Vorjahren, nämlich Abgeordnete und Führungskräfte aus großen Unternehmen, als Basis, so liegt der Anteil derjenigen, die das Cloud Computing für sicher halten, heute mit

27 Prozent über dem Niveau von 2011 und 2012, als 21 bzw. 23 Prozent diese IT-Lösung als sicher einstufen. Nach wie vor überwiegt gleichwohl – trotz der steigenden Inanspruchnahme von Cloud Services – auch in dieser Gruppe der Anteil derjenigen, die das Cloud Computing als unsicher einstufen, deutlich (Tabelle 5).

Tabelle 5

Einstellung zum Cloud Computing im Zeitverlauf

Cloud Computing ist –	Abgeordnete und Führungskräfte in großen Unternehmen		
	2011 %	2012 %	2013 %
sehr sicher	2	2	2
eher sicher	19	21	25
eher unsicher	47	49	48
sehr unsicher	26	19	20

Auf 100 fehlende Prozent: kommt darauf an, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in großen Unternehmen · Quelle: Allensbacher Archiv, IfD-Umfragen 6220, 6240 und 6267 (Juni/Juli 2013)

IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN

Der Aufgabenkatalog für die Politik im Bereich der IT-Sicherheit ist umfangreich. Von den zur Diskussion gestellten Aufgaben werden alle von drei Vierteln und mehr der Entscheider aus Politik und Wirtschaft als sehr wichtig oder wichtig eingestuft. Abgeordnete und Führungskräfte in den Unternehmen weisen dabei eine erstaunliche Übereinstimmung bei den Prioritäten auf. Fokussiert man auf die höchste Antwortkategorie „sehr wichtig“, nehmen der Schutz der kritischen physischen Infrastrukturen wie Verkehrswege oder Energieversorgung sowie die stärkere internationale Zusammenarbeit beim Thema IT-Sicherheit eine herausragende Rolle ein. 67 Prozent der Führungskräfte aus den Unternehmen und 70 Prozent der Abgeordneten sehen im Schutz der öffentlichen Infrastruktur vor IT-Angriffen eine sehr wichtige Aufgabe der Politik. Die stärkere internationale Zusammenarbeit beim Thema IT-Sicherheit gilt 56 Prozent der Führungskräfte und 66 Prozent der Abgeordneten als besonders wichtig.

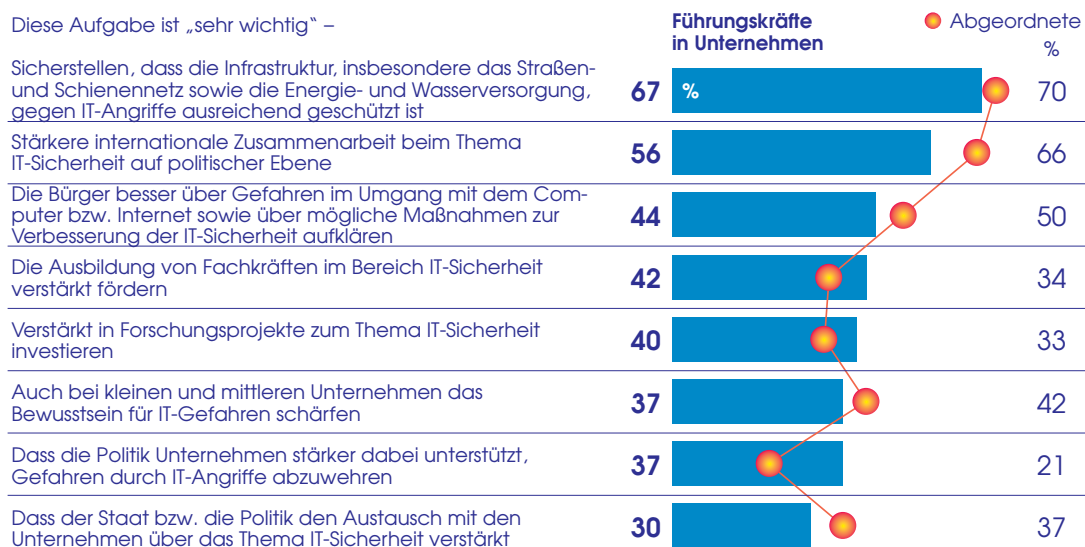
An dritter Stelle steht für Führungskräfte in der Wirtschaft wie für Abgeordnete die stärkere Sensibilisierung und Aufklärung der Bürger in Bezug auf Risiken im Umgang mit Computer und Internet. Gefolgt von der verstärkten Förderung der Ausbildung von IT-Fachkräften und der stärkeren Investition in Forschungsprojekte zum Thema IT-Sicherheit.

Eine der wenigen Aufgaben, bei der es gravierende Unterschiede zwischen der Einschätzung von Abgeordneten und Führungskräften aus der Wirtschaft gibt, ist die stärkere Unterstützung der Unternehmen durch die Politik, Gefahren, die von IT-Angriffen ausgehen, abzuwehren. Während von den Abgeordneten nur 21 Prozent dies als besonders wichtige Aufgabe für die Politik sehen, sind es in der Wirtschaft 37 Prozent (Schaubild 25).

Schaubild 25

Die wichtigsten Aufgaben für die Politik im Bereich IT-Sicherheit

Frage: „Zum Thema IT-Sicherheit: Was sind Ihrer Ansicht nach die wichtigsten Aufgaben, die die Politik im Bereich IT-Sicherheit angehen sollte? Ist die jeweilige Aufgabe sehr wichtig, wichtig, weniger wichtig oder gar nicht wichtig?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN

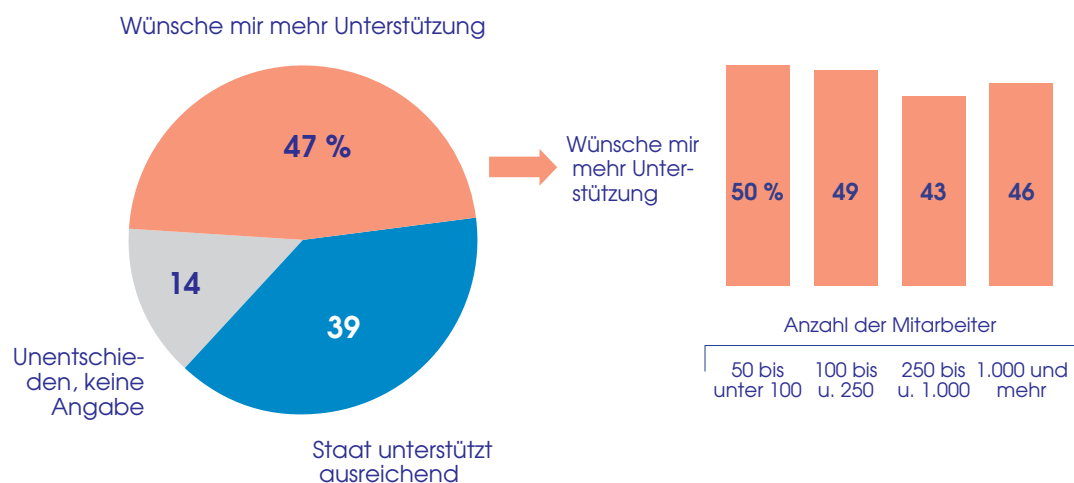
47 Prozent der Unternehmen wünschen sich bei der Bekämpfung von IT-Angriffen mehr Unterstützung durch den Staat, 39 Prozent halten die gegenwärtige Unterstützung für ausreichend.

Die Forderung nach mehr Unterstützung ist dabei weitgehend unabhängig von der Unternehmensgröße und schwankt zwischen 43 und 50 Prozent (Schaubild 26).

Schaubild 26

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?“



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Um die vielfältigen staatlichen Aufgaben im Bereich der IT-Sicherheit effektiv angehen zu können, bedarf es bei Gesetzgeber wie Verwaltung ausreichender Fachkompetenz. Allerdings konstatieren sowohl die Führungskräfte aus der Wirtschaft als auch die Abgeordneten selbst, dass die erforderliche Fachkompetenz beim Thema IT-Sicherheit – im Gegensatz zu anderen Politikfeldern – derzeit bei der öffentlichen Hand nicht vorhanden ist. Dabei wird die staatliche Kompetenz in allen Bereichen von den Führungskräften in den Unternehmen kritischer bewertet als von den Abgeordneten. So halten 74 Prozent der Abgeordneten die Fachkompetenz von Regie-

rung, Parlamenten und Behörden im Bereich der Nutzung der Kernenergie für ausreichend, von den Führungskräften aus der Wirtschaft sind es 61 Prozent. Ähnlich viele sind es mit 72 bzw. 55 Prozent bei der Lebensmittelsicherheit. Bei der Verbrechensbekämpfung sind 80 Prozent der Abgeordneten, aber nur 46 Prozent der Führungskräfte aus der Wirtschaft von der Fachkompetenz der staatlichen Funktionsträger überzeugt. Ein gänzlich anderes Bild zeigt sich bei der IT-Sicherheit. Nur eine Minderheit sowohl der Abgeordneten als auch der Führungskräfte in den Unternehmen attestiert Politik und Verwaltung ein ausreichendes Know-how. Von den Abgeordneten

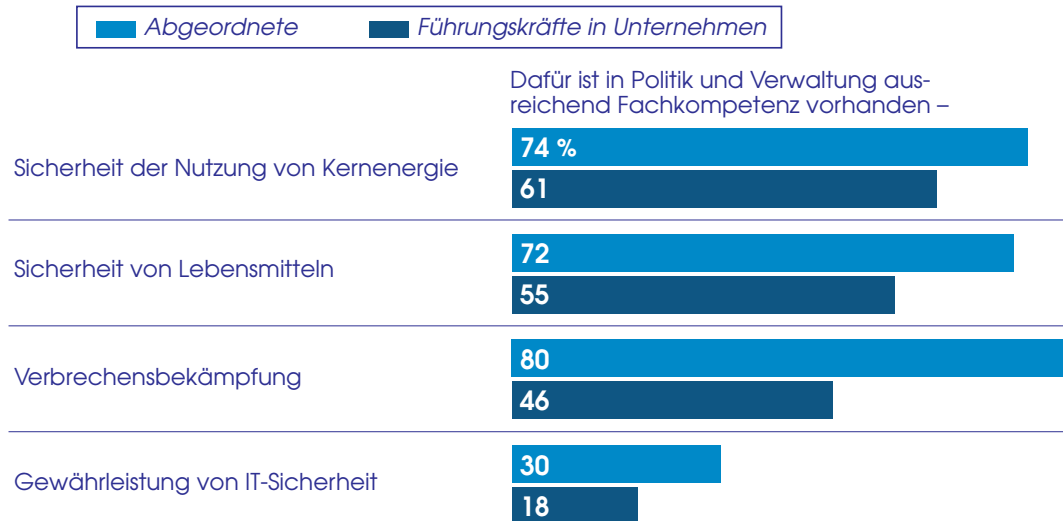
sind es 30 Prozent, von den Führungskräften in den Unternehmen gerade einmal 18 Prozent, die davon überzeugt sind, dass es auf staatlicher Seite genügend Fachkompetenz für die Schaf-

fung gesetzlicher Rahmenbedingungen zur Gewährleistung von IT-Sicherheit gibt (Schaubild 27).

Schaubild 27

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 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN

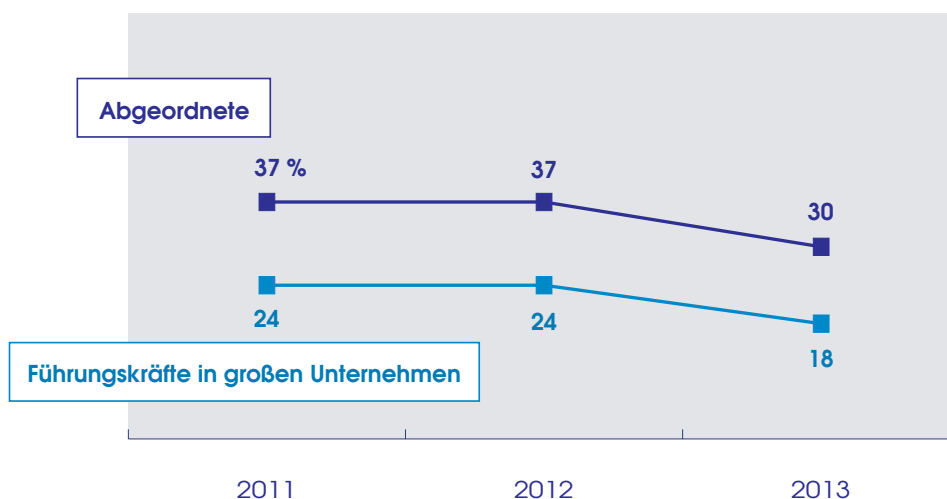
Im Vergleich zu den Vorjahren wird die staatliche Fachkompetenz sowohl von Abgeordneten wie von Führungskräften in großen Unternehmen als schlechter eingestuft. Bewerteten in den letzten beiden Jahren jeweils 37 Prozent der Abgeordneten und 24 Prozent der Führungskräfte aus großen Unterneh-

men die Fachkompetenz staatlicher Stellen für die Schaffung gesetzlicher Rahmenbedingungen im Bereich der IT-Sicherheit mit ausreichend, ist der Anteil in diesen beiden Personengruppen binnen der letzten 12 Monate auf 30 bzw. 18 Prozent gesunken (Schaubild 28).

Schaubild 28

Fachkompetenz in Politik und Verwaltung wird schlechter bewertet als in den letzten Jahren

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



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfragen 6220, 6240 und 6267 (Juni/Juli 2013)

© IfD-Allensbach

Die Politik sieht aber nicht nur bei der eigenen Fachkompetenz Defizite. Sie sieht auch Versäumnisse bei den Unternehmen. Nur 11 Prozent der Politiker sind der Meinung, dass die Unternehmen in Deutschland bestmöglich auf Gefahren für ihre IT-Systeme vorbereitet sind. 38 Prozent sehen die Unternehmen zumindest einigermaßen vorbereitet. 44 Prozent ha-

ben jedoch auch daran Zweifel. Diese Einschätzung steht in scharfem Kontrast zur Selbsteinschätzung der Unternehmen.⁶ Denn 56 Prozent der Führungskräfte sehen ihr eigenes Unternehmen bestmöglich auf eventuelle Gefahren für die IT-Sicherheit vorbereitet, nur 9 Prozent haben Zweifel daran, gut oder zumindest einigermaßen vorbereitet zu sein (Schaubild 29).

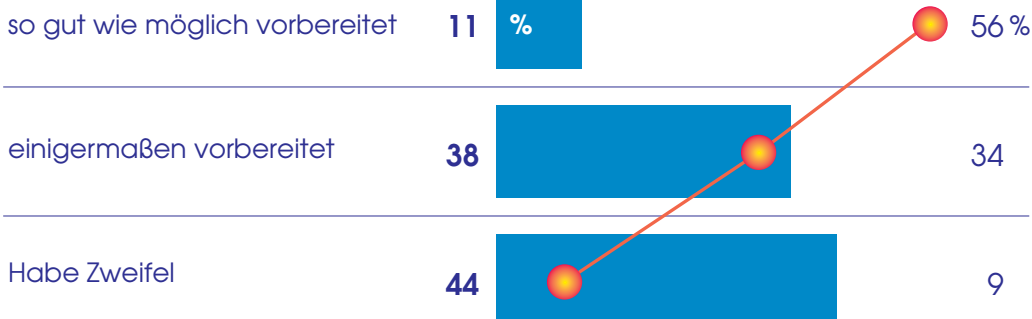
Schaubild 29

Skepsis unter den Politikern, ob Unternehmen auf die Gefahren für die IT-Sicherheit ausreichend vorbereitet sind

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?“

Aus Sicht der Politiker sind die Unternehmen in Deutschland auf Gefahren für die IT-Sicherheit –

Zum Vergleich:
Die Führungskräfte sehen ihr **eigenes** Unternehmen –



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

⁶Vgl. auch Schaubild 14.

IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN

Trotz der skeptischen Bewertung, inwiefern bei Gesetzgeber und Verwaltung ausreichend Fachkompetenz im Bereich IT-Sicherheit vorhanden ist: In weiten Teilen haben die Abgeordneten durchaus ein gutes Gespür dafür, in welchen Bereichen auf Unternehmensseite der größte Handlungsbedarf besteht und welches die größten Gefahrenquellen für die IT-Sicherheit in den Unternehmen sind. So nennen die Abgeordneten bei der offenen Abfrage – also ohne Antwortvorgaben – weitgehend die gleichen Punkte als besonders wichtige Handlungsfelder wie die Führungskräfte in Unternehmen: Schulung, Information und Sensibilisierung von Mitarbeitern geben 17 Prozent der Politiker spontan als größten Handlungsbedarf an, 13 Prozent den Schutz vor IT-Angriffen von außen. Von den Führungskräften in den Unternehmen nannten 23 Prozent bzw. 12 Prozent diese Themen als besonders wichtig. Auch die funktionierenden

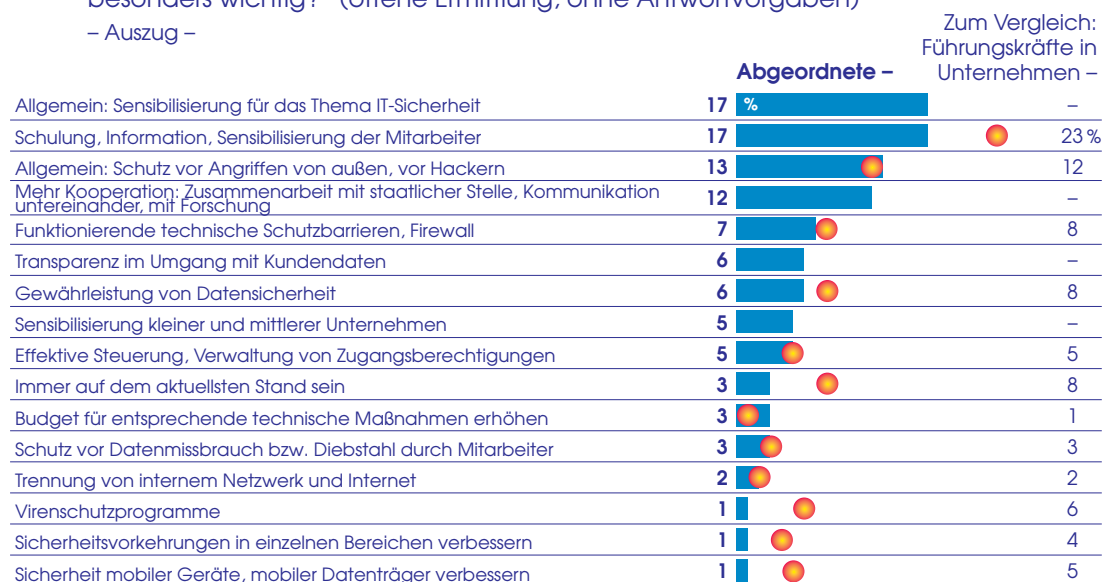
technischen Schutzbarrieren sowie die Gewährleistung von Datensicherheit sind Themen, die von Abgeordneten wie Führungskräften ähnlich häufig genannt wurden. Von den Abgeordneten wurden zudem einige allgemeine Aspekte ins Feld geführt, die von den Führungskräften angesichts der leicht anderen, auf ihr eigenes Unternehmen zugeschnittenen Fragestellung nicht erwähnt wurden. Dazu zählen mit 17 Prozent die Sensibilisierung für das Thema IT-Sicherheit allgemein sowie mit 12 Prozent die stärkere Kooperation: mit staatlichen Stellen, zwischen den Unternehmen, aber auch mit der Forschung. Die Transparenz im Umgang mit Kundendaten ist ebenfalls ein Punkt, der von den Unternehmen nicht genannt wurde, für die Abgeordneten aber durchaus eine Rolle spielt (Schaubild 30).

Schaubild 30

Handlungsbedarf bei der IT-Sicherheit in den Unternehmen – aus Sicht der Politik

Frage: „Wenn Sie einmal an die IT-Sicherheit denken: Wo sehen Sie da bei den Unternehmen in Deutschland ganz allgemein den größten Handlungsbedarf, was halten Sie für besonders wichtig?“ (offene Ermittlung, ohne Antwortvorgaben)

– Auszug –



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Bei den Gefahrenquellen gibt es ebenfalls teilweise ähnliche Einschätzungen, mitunter jedoch auch erhebliche Unterschiede in der Bewertung der einzelnen Gefahrenquellen. Generell schätzen die Abgeordneten das Risikopotenzial aller Gefahrenquellen als deutlich höher ein, als die Führungskräfte dies für ihr eigenes Unternehmen tun. Beim Gefährdungspotenzial, das vom leichtfertigen Umgang der Mitarbeiter mit Daten oder Sicherheitsbestimmungen oder im Hinblick auf die Nutzung mobiler Endgeräte ausgeht, ergibt sich allerdings durchaus ein ähnliches Bild. 71 Prozent der Abgeordneten sehen im leichtfertigen Umgang der Mitarbeiter mit Daten oder Sicherheitsbestimmungen eine sehr große oder große Gefahr für die IT-Sicherheit deutscher Unternehmen. Für das eigene Unternehmen sehen darin 57 Prozent der Führungskräfte aus der Wirtschaft eine sehr große oder große Gefahr. Und auch die

Nutzung mobiler Endgeräte wird von 64 Prozent der Abgeordneten sowie 50 Prozent der Führungskräfte in ähnlichem Maße als Risikoquelle gesehen. Nennenswerte Unterschiede gibt es indes bei der Bewertung von Hackerangriffen. So geht aus Sicht von 79 Prozent der Abgeordneten von Hackerangriffen eine sehr große oder große Gefahr für die IT-Sicherheit in deutschen Unternehmen aus. Für die Führungskräfte spielt diese Bedrohung aber eine eher nachrangige Rolle für die IT-Sicherheit in ihrem Unternehmen. Und auch beim Einsatz veralteter Technik und beim Datenmissbrauch gehen die Bewertungen von Abgeordneten und Führungskräften signifikant auseinander (Schaubild 31).

Schaubild 31

Gefahrenquellen für die IT-Sicherheit in deutschen Unternehmen aus Sicht der Politik

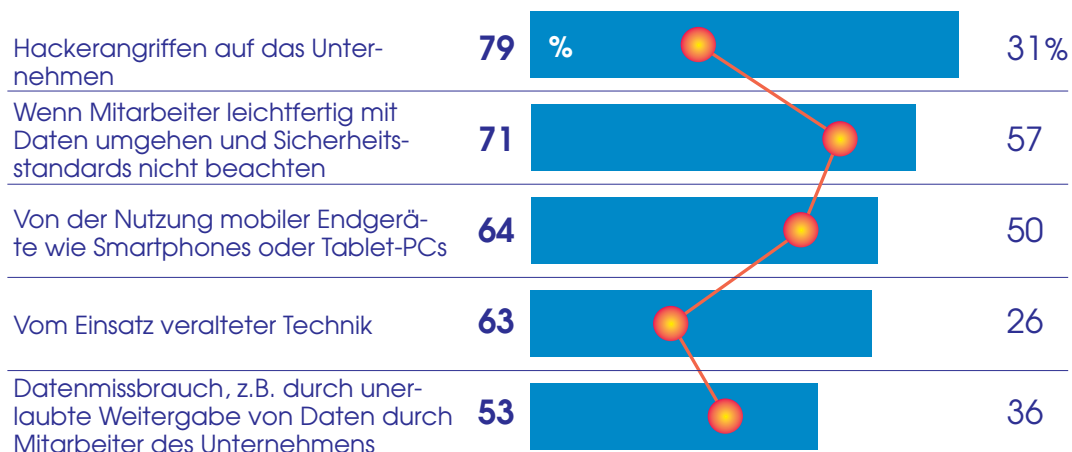
Frage: „Wovon geht Ihrer Meinung nach eine sehr große, eine große, eine weniger große oder kaum eine Gefahr aus?“

– Auszug –

Davon geht eine sehr große oder große Gefahr aus –

Abgeordnete

Zum Vergleich: Gefahrenquellen für das **eigene** Unternehmen aus Sicht von Führungskräften in Unternehmen



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN

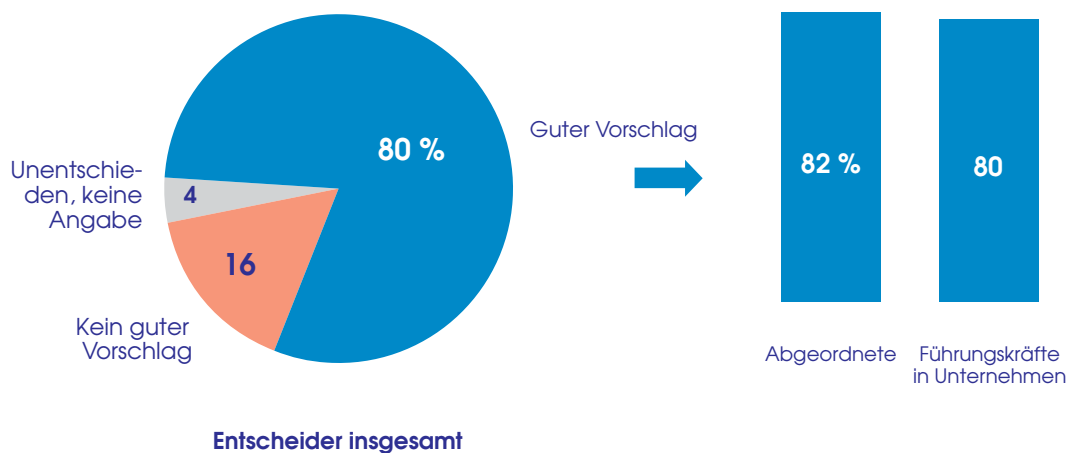
Nach den im Frühjahr vorgestellten Plänen der EU-Kommission sollen künftig Unternehmen aus bestimmten Branchen Hackerangriffe melden müssen. Vor diesem Hintergrund wurden die Entscheider aus Politik und Wirtschaft um ihre Meinung gebeten, ob sie die Meldung von Hackerangriffen an eine zentrale Stelle grundsätzlich begrüßen würden oder eher skeptisch sehen. Die Ergebnisse signalisieren eine im Grundsatz breite Zustimmung. 80 Prozent finden den Vorschlag gut, nur

16 Prozent halten die Meldung von Hackerangriffen an eine zentrale Stelle für keinen guten Vorschlag. Die Zustimmung ist sowohl unter Abgeordneten wie unter Führungskräften in den Unternehmen mit 82 bzw. 80 Prozent ähnlich stark ausgeprägt (Schaubild 32).

Schaubild 32

Breite Zustimmung für eine zentrale Meldung von Hackerangriffen

Frage: „Was halten Sie von dem Vorschlag, dass Unternehmen Hackerangriffe an eine zentrale Stelle melden sollen: Halten Sie das grundsätzlich für einen guten oder keinen guten Vorschlag?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

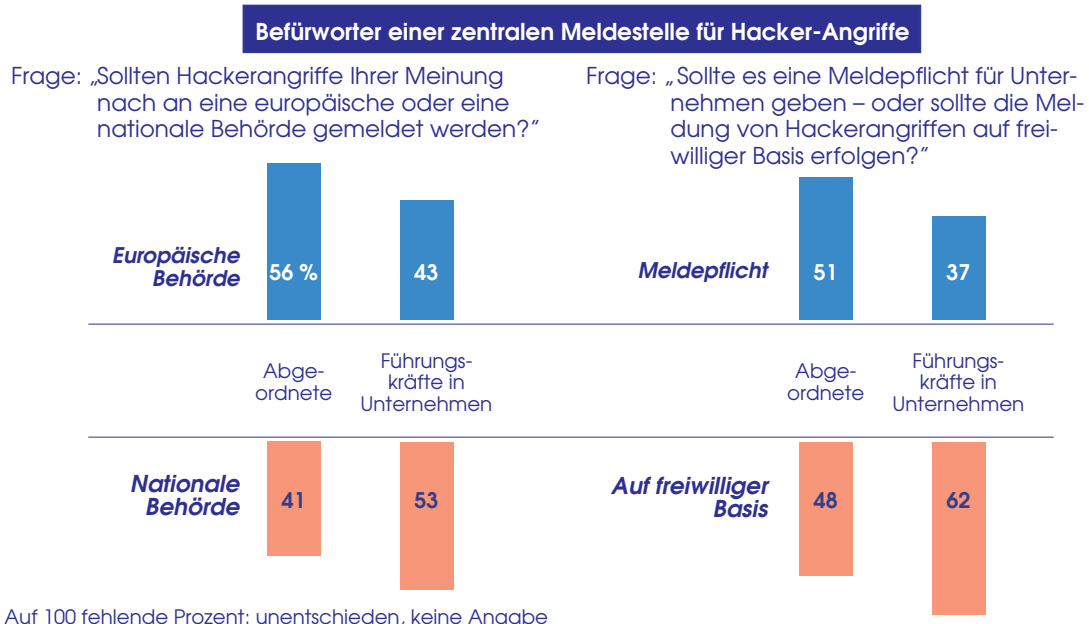
© IfD-Allensbach

Bei den Umsetzungsoptionen für eine solche zentrale Meldestelle für Hackerangriffe gehen die Auffassungen jedoch auseinander. So plädieren von den Abgeordneten, die den Vorschlag grundsätzlich gut finden, 56 Prozent für eine europäische Behörde. Unter den Führungskräften aus den Unternehmen, die den Vorschlag befürworten, spricht sich die Mehrheit (53 Prozent) für eine nationale Behörde aus. Auch bei der Frage, ob es eine Meldepflicht geben sollte oder die Meldungen auf freiwilliger

Basis erfolgen sollten, gehen die Meinungen auseinander. Bei den Abgeordneten halten sich beide Optionen mit 51 bzw. 48 Prozent weitgehend die Waage. Die Führungskräfte befürworten mehrheitlich eine Meldung auf freiwilliger Basis. Von denjenigen Führungskräften, die eine zentrale Behörde grundsätzlich gut finden, wünschen sich 62 Prozent eine Lösung, die auf eine freiwillige Meldung der Hackerangriffe setzt; 37 Prozent befürworten eine Meldepflicht (Schaubild 33).

Schaubild 33

Uneinheitliches Meinungsbild hinsichtlich der operativen Fragen zur Umsetzung einer zentralen Meldestelle für Hackerangriffe



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen, die den Vorschlag einer zentralen Meldung von Hackerangriffen gut finden
 Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

IT-SICHERHEIT: VIELE AUFGABEN FÜR DIE POLITIK, ABER ZUNEHMENDE ZWEIFEL AN DER KOMPETENZ VON POLITIK UND BEHÖRDEN

Diejenigen, die die zentrale Meldung von Hackerangriffen an eine staatliche Stelle für keinen guten Vorschlag halten, begründen dies vor allem damit, dass der Aufwand den Nutzen übersteigen würde. Bezogen auf alle Entscheider, nennen 11 Prozent dies als Grund. 4 Prozent nennen als Grund für ihre ablehnende

Haltung, dass eine solche zentrale Meldung für Unternehmen in der Praxis nur schwer umsetzbar sei. 3 Prozent geben zu bedenken, dass der Ruf des Unternehmens darunter leiden könnte (Tabelle 6).

Tabelle 6

Gründe für eine ablehnende Haltung zu einer zentralen Meldestelle für Hackerangriffe

FRAGE: „Was halten Sie von dem Vorschlag, dass Unternehmen Hackerangriffe an eine zentrale Stelle melden sollen: Halten Sie das grundsätzlich für einen guten oder keinen guten Vorschlag?“

Falls ‚kein guter Vorschlag‘: „Warum halten Sie das für keinen guten Vorschlag: weil es in der Praxis für Unternehmen nur schwer umsetzbar ist, weil der Aufwand einer solchen Regelung den Nutzen übersteigt, weil der Ruf von Unternehmen darunter leiden könnte, oder warum sonst?“

	Entscheider insgesamt %
Es finden den Vorschlag nicht gut	16
Aufwand übersteigt Nutzen	11
Nur schwer umsetzbar	4
Ruf des Unternehmens könnte leiden	3
Anderes	3
Es finden den Vorschlag gut	80
Unentschieden, keine Angabe	4

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

Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

UNTERNEHMENSÜBERGREIFENDE INITIATIVEN WERDEN FÜR WICHTIG GEHALTEN – BISLANG IST ABER NUR EINE MINDERHEIT DER UNTERNEHMEN IN INITIATIVEN ZUM THEMA IT-SICHERHEIT EINGEBUNDEN

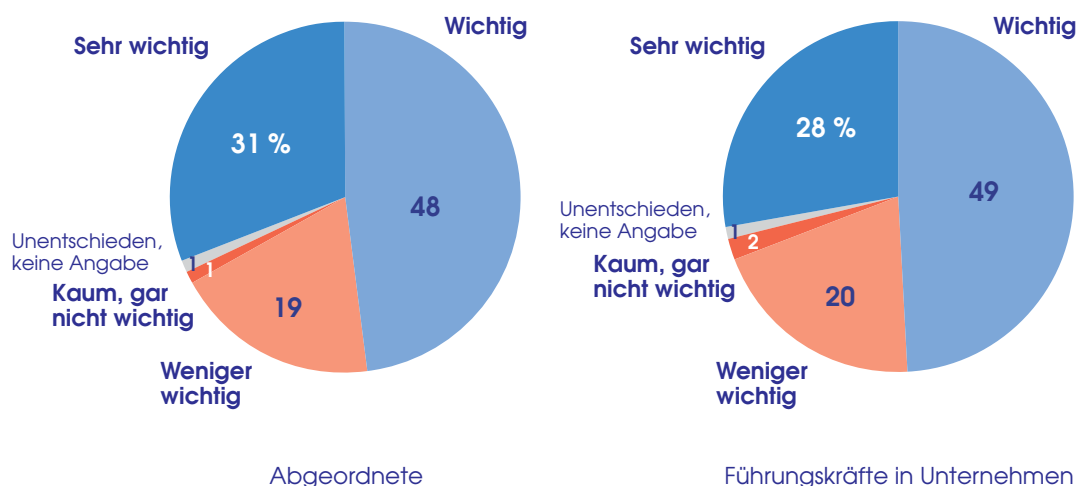
Neben dem Ruf nach staatlichen Maßnahmen zur Bekämpfung von IT-Angriffen ist aus Sicht der Entscheider aus Politik und Wirtschaft zudem der stärkere Austausch zwischen den Unternehmen selbst wichtig, um IT-Angriffen künftig besser vorbeugen zu können. 31 Prozent der Abgeordneten finden

diesen unternehmensübergreifenden Dialog sehr wichtig, weitere 48 Prozent wichtig. Die Führungskräfte aus den Unternehmen selbst halten den Austausch untereinander für ähnlich wichtig: 28 Prozent finden ihn sehr wichtig, 49 Prozent wichtig (Schaubild 34).

Schaubild 34

Stärkerer Austausch zwischen Unternehmen zur Vorbeugung gegen IT-Angriffe

Frage: „Für wie wichtig halten Sie es, dass sich deutsche Unternehmen untereinander stärker austauschen, um IT-Angriffen vorzubeugen? Halten Sie das für sehr wichtig, wichtig, weniger wichtig oder kaum, gar nicht wichtig?“



Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

UNTERNEHMENSÜBERGREIFENDE INITIATIVEN WERDEN FÜR WICHTIG GEHALTEN – BISLANG IST ABER NUR EINE MINDERHEIT DER UNTERNEHMEN IN INITIATIVEN ZUM THEMA IT-SICHERHEIT EINGEBUNDEN

Der Wunsch nach einem stärkeren Austausch zwischen Unternehmen, aber auch mit staatlichen Stellen, lässt sich nicht zuletzt durch den großen volkswirtschaftlichen Schaden erklären, der aus Sicht der Entscheider aus Politik und Wirtschaft der deutschen Wirtschaft jedes Jahr durch IT-Angriffe entsteht. Von den Abgeordneten halten 73 Prozent den Schaden für sehr groß oder groß: 29 Prozent halten ihn für sehr groß, 44

Prozent für groß. Von den Führungskräften in den Unternehmen sind sogar 82 Prozent der Meinung, dass der Schaden sehr groß (37 Prozent) oder groß (45 Prozent) ist. Nur 20 Prozent der Abgeordneten und 14 Prozent der Führungskräfte aus der Wirtschaft stufen den Schaden als weniger groß oder sehr gering ein (Schaubild 35).

Schaubild 35

Hoher Schaden durch IT-Angriffe

Frage: „Wie groß ist Ihrer Einschätzung nach der Schaden für die deutsche Wirtschaft, der jedes Jahr durch IT-Angriffe entsteht?“

Der Schaden ist –

„sehr groß“

29 %

37

„groß“

44

45

„weniger groß“

20

14

„sehr gering“

6

3

Unentschieden, keine Angabe

Abgeordnete

Führungskräfte
in Unternehmen

Basis: Bundesrepublik Deutschland, Abgeordnete und Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

Derzeit ist nur ein kleiner Teil der mittleren und großen Unternehmen in Initiativen zum Thema IT-Sicherheit eingebunden. 2 Prozent der Unternehmen sind darin sehr stark, 11 Prozent stark involviert. Die ganz überwiegende Mehrheit ist jedoch nur in geringem Maße oder gar nicht eingebunden. Am ehes-

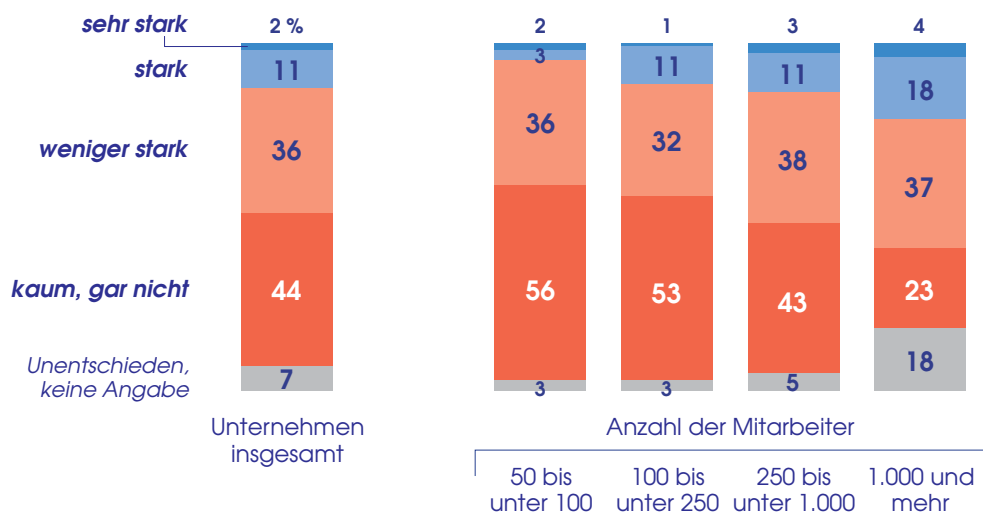
ten noch sind große Unternehmen mit 1.000 und mehr Mitarbeitern Teil solcher Initiativen. Von ihnen ist gut jedes fünfte Unternehmen in eine derartige Initiative involviert (Schaubild 36).

Schaubild 36

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 –



Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen

Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

UNTERNEHMENSÜBERGREIFENDE INITIATIVEN WERDEN FÜR WICHTIG GEHALTEN – BISLANG IST ABER NUR EINE MINDERHEIT DER UNTERNEHMEN IN INITIATIVEN ZUM THEMA IT-SICHERHEIT EINGEBUNDEN

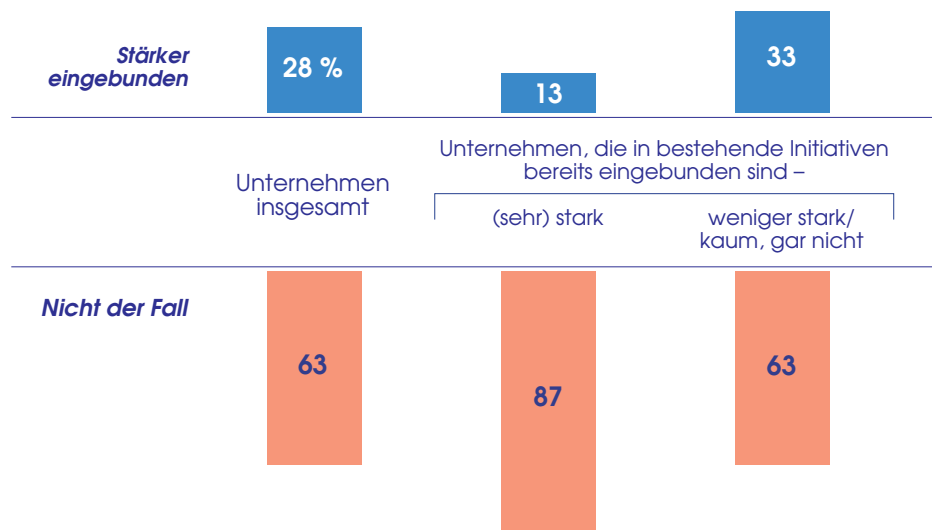
Der Wunsch nach einer stärkeren Einbindung ist dabei unterschiedlich stark ausgeprägt. Insgesamt würden sich 28 Prozent der Unternehmen wünschen, stärker in solche Initiativen zur IT-Sicherheit eingebunden zu sein; 63 Prozent sehen hier keinen Bedarf. Von den Unternehmen, die derzeit bereits sehr stark oder stark eingebunden sind, sind nur 13 Prozent

an einer noch stärkeren Einbindung interessiert. Von den bislang weniger stark oder gar nicht involvierten Unternehmen würde sich jedoch immerhin jedes dritte wünschen, künftig stärker in Initiativen zur IT-Sicherheit einbezogen zu sein (Schaubild 37).

Schaubild 37

Unterschiedlich ausgeprägter 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 6267 (Juni/Juli 2013)

© IfD-Allensbach

Aus Sicht der Unternehmen sollten bei Initiativen zur IT-Sicherheit vor allem operative Themen im Mittelpunkt stehen. 65 Prozent der Führungskräfte aus mittleren und großen Unternehmen wünschen sich den Austausch über Best-Practice-Ansätze im Rahmen solcher Initiativen, 43 Prozent erhoffen sich ein besseres Verständnis der Bedrohungslage. Nur 16 Prozent

der Führungskräfte sehen den vorrangigen Zweck solcher Initiativen darin, als Plattform für eine Diskussion darüber zu dienen, wo bei Politik und Behörden der größte Handlungsbedarf besteht (Schaubild 38).

Schaubild 38

Fokus der Initiativen sollte auf operativen Themen liegen

Frage: „Worum sollte es Ihrer Meinung nach bei solchen Initiativen vor allem gehen, was sollte im Mittelpunkt stehen: eine Diskussion darüber, wo Handlungsbedarf für Politik und Behörden besteht, oder der Austausch von Best-Practice-Ansätzen bei der Bekämpfung von IT-Angriffen, oder ein besseres Verständnis der aktuellen Bedrohungslage, oder was sonst?“ (Mehrfachangaben möglich)

Bei den Initiativen sollte im Mittelpunkt stehen –

Austausch von Best-Practice-Ansätzen

65

%

Besseres Verständnis der Bedrohungslage

43

Diskussion über Handlungsbedarf für Politik und Behörden

16

Anderes

1

Basis: Bundesrepublik Deutschland, Führungskräfte in mittleren und großen Unternehmen
Quelle: Allensbacher Archiv, IfD-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

UNTERNEHMENSÜBERGREIFENDE INITIATIVEN WERDEN FÜR WICHTIG GEHALTEN – BISLANG IST ABER NUR EINE MINDERHEIT DER UNTERNEHMEN IN INITIATIVEN ZUM THEMA IT-SICHERHEIT EINGEBUNDEN

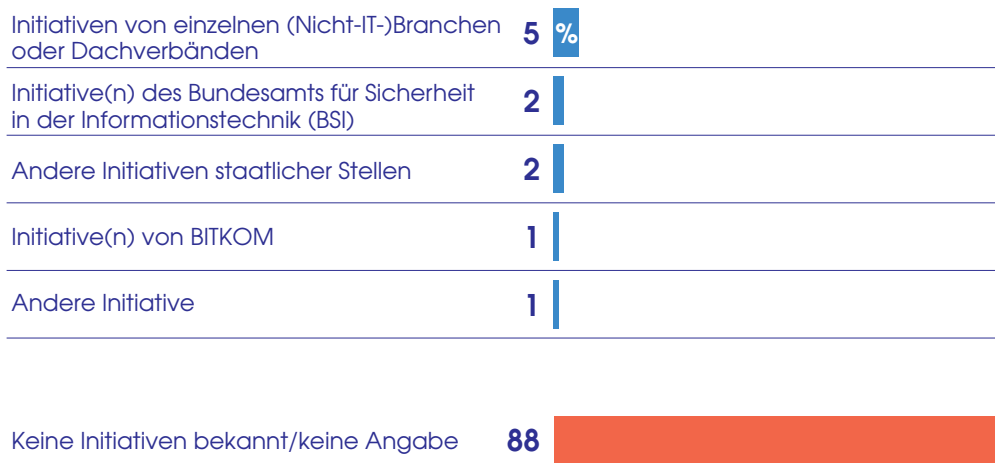
Die wenigsten Führungskräfte können konkrete Initiativen aus dem Bereich IT-Sicherheit benennen. Auf die offene Frage (ohne Antwortvorgaben), welche Initiativen ihnen in diesem Bereich bekannt sind, machen 88 Prozent der Führungskräfte keine Angabe. Am ehesten noch sind Initiativen von einzelnen Branchen oder Dachverbänden außerhalb der IT-Branche bekannt. 5 Prozent der Führungskräfte nannten Initiativen aus

diesem Bereich. Initiativen des Bundesamts für Sicherheit in der Informationstechnik werden von 2 Prozent angegeben. Aktivitäten anderer staatlicher Stellen wurden von ebenfalls 2 Prozent spontan erwähnt. Die Initiativen des IT-Branchenverbands BITKOM kennt 1 Prozent. 1 Prozent der Führungskräfte nennt zudem andere Initiativen, die keinem der vorgenannten Akteure zuzuordnen sind (Schaubild 39).

Schaubild 39

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-Umfrage 6267 (Juni/Juli 2013)

© IfD-Allensbach

ANHANG: STUDIENDESIGN IM ÜBERBLICK

STICHPROBE:

a) 117 Abgeordnete, davon

44 Bundestagsabgeordnete,
59 Landtagsabgeordnete und
14 deutsche Abgeordnete im EU-Parlament

b) 514 Führungskräfte aus mittleren und großen Unternehmen, davon

293 Führungskräfte aus mittleren Unternehmen,
221 Führungskräfte aus Großunternehmen,

296 Inhaber, Geschäftsführer oder Vorstände und
218 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 Mitarbeitern haben und/oder einen Jahresumsatz von 10 bis höchstens 50 Mio. Euro erzielen.

METHODE:

Telefonische Interviews (CATI)

BEFRAGUNGSZEITRAUM:

5. Juni bis 15. Juli 2013