Cyber Security Report 2012

Ergebnisse einer repräsentativen Befragung
von Entscheidungsträgern aus Wirtschaft und Politik

INHALT

Herausgeber:
Deutsche Telekom/T-Systems

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

Centrum für Strategie und Höhere Führung
Bodman am Bodensee

Ansprechpartner:
Harald Lindlar
harald.lindlar@telekom.de
Prof. Dr. Klaus Schweinsberg
klaus.schweinsberg@glh-online.com

VORWORT

Die Angst vor Angriffen im und aus dem Cyberspace wächst. Immer mehr Entscheidungsträger aus Wirtschaft und Politik sind beunruhigt. Das zeigen die Ergebnisse der repräsentativen Umfrage des Instituts für Demoskopie Allensbach unter Entscheidungsträgern aus der Wirtschaft sowie Landtags-, Bundestags- und EU-Abgeordneten. 80 Prozent sind der Meinung, Wirtschafts- und Industriespionage richte in der deutschen Wirtschaft schon heute großen Schaden an. Für diese Spionage nutzen die Diebe immer häufiger den Cyberspace. Daher glauben viele Entscheidungsträger, dass das Missbrauchsrisiko von persönlichen Daten sowie auch das Risiko von Internet- und Computerkriminalität in Zukunft weiter stark zunehmen wird.

Die Werkzeuge der virtuellen Angreifer sind äußerst raffiniert. Sie sind unsichtbar und ihre Herkunft ist kaum zu identifizieren. Sie verändern sich ständig, decken immer wieder neue Sicherheitslücken auf und machen es daher so schwer, sich gegen sie zur Wehr zu setzen. Es sind nicht so sehr die bekannten Viren, Würmer und Trojaner auf PCs und mobilen Endgeräten, die beunruhigen. Es sind hochgradig intelligente Angriffsprogramme wie Stuxnet, Duqu und Flame, die einen regelrechten Cyberwar entfachen können. Experten jedenfalls nennen diese professionellen Spionagewerkzeuge der vierten Generation „Kriegsmittel". Sie führen Sabotage und Spionage in ganz neue Dimensionen. Wirtschaft und Staat haben nur dann eine Chance, wenn sie sich gemeinsam zur Wehr setzen, sich austauschen und zusammenarbeiten. Nur wer schnell agiert und seine Abwehrtechnik permanent verbessert, wird sich auf Dauer gegen Cyberkriminelle durchsetzen können.

Das alles mag nach Zukunft, nach Panikmache, nach Hysterie klingen. Aber alle Zeichen deuten darauf hin, dass sich in einer zunehmend stärker vernetzten Gesellschaft die Angriffe auf Daten, Unternehmenswerte und Geld immer mehr ins Netz verlagern. Die Zahl der politisch oder ökonomisch motivierten Raubzüge im Netz wird rasch steigen. Dies trifft inzwischen alle Branchen, wie einige Beispiele aus den vergangenen Wochen zeigen. Eine unbekannte Hacker-Gruppe hat den saudi-arabischen Ölkonzern Saudi Aramco attackiert, einen Virus in das Firmennetz eingeschleust und damit 30.000 Computer lahmgelegt. Ein digitaler Schädling mit dem Namen „Gauss" hat im Nahen Osten Banktransaktionen ausgespäht. Ein ehemaliger Mitarbeiter von Toyota USA hat Webanwendungen und Sicherheitssysteme sabotiert und streng vertrauliche Daten heruntergeladen. Das macht deutlich: Der Feind lauert auch in den eigenen Reihen.

Gegen die Waffen des Cyberwars kommen IT-, Netz- und Sicherheitsspezialisten allein nicht mehr an. Dringend notwendig ist eine übergreifende Allianz gegen die virtuelle Bedrohung: Regierungen, Unternehmen, IT-Dienstleister und Telekommunikationsanbieter müssen enger zusammenarbeiten und sich besser vernetzen als bisher. Ansätze hierzu existieren. Zu einer gesamtheitlichen Sicherheitsstrategie gehören zudem Frühwarnsysteme, die alle Parteien im Netzwerk über das Aufziehen eines digitalen Tsunamis informieren. Denn letztlich weiß niemand, wann und wo der nächste Angriff erfolgt. Darum müssen wir alle Kräfte bündeln. Das sehen laut Cyber Security Report die Entscheidungsträger genauso: 87 Prozent der Befragten halten den Dialog zwischen den Unternehmen für wichtig oder sogar sehr wichtig. Nur so lässt sich die Gefahr aus dem Netz, wenn schon nicht verhindern, dann wenigstens wirksam eindämmen.

Reinhard Clemens
Vorstand Deutsche Telekom und CEO T-Systems

EINFÜHRUNG

Im Jahr 2011 hat das Institut für Demoskopie Allensbach im Auftrag von T-Systems in Kooperation mit dem Centrum für Strategie und Höhere Führung erstmals einen Sicherheitsreport erstellt. Im Rahmen dieses Sicherheitsreports wurde auch die Risikoeinschätzung von Entscheidungsträgern aus Wirtschaft und Politik untersucht. Angesichts der Vielzahl von Risiken, die durch das Internet für Privatpersonen, aber auch für Staaten und Unternehmen, beispielsweise durch den offensiven Einsatz moderner Cyberwar-Instrumente wie Stuxnet oder Flame, ausgehen, wurde in diesem Jahr ein spezieller „Cyber Security Report" erstellt.

Im Mittelpunkt des Cyber Security Reports stehen IT- und Datenschutzrisiken. Zunächst wurde untersucht, welches Risikopotenzial Entscheidungsträger diesen Gefahren im Vergleich zu Risiken in anderen Lebensbereichen beimessen. Anschließend lag der Schwerpunkt unter anderem auf dem Stellenwert der IT-Sicherheit im eigenen Unternehmen, der Bewertung von Hacker-Angriffen sowie den getroffenen Maßnahmen zum Schutz vor solchen Angriffen, den Einschätzungen zu Wirtschafts- und Industriespionage sowie zur Fachkompetenz der Exekutive auf verschiedenen sicherheitsrelevanten Politikfeldern.

Die Untersuchung stützt sich auf 342 Interviews mit einem repräsentativen Querschnitt von Entscheidungsträgern aus Wirtschaft und Politik, darunter 128 Interviews mit Abgeordneten aus Bundestag, Landtagen und deutschen Abgeordneten aus dem Europaparlament sowie 214 Interviews mit Top-Führungskräften aus der Wirtschaft, also z. B. Geschäftsführern, Vorständen oder Bereichsleitern in großen Unternehmen aller Branchen. Als Großunternehmen gelten gemäß der Definition der EU-Kommission Unternehmen mit mindestens 250 Beschäftigten oder einem Jahresumsatz von mehr als 50 Millionen Euro. Die telefonischen Interviews wurden im Juni und Juli 2012 durchgeführt. Die detaillierten Untersuchungsdaten sind im Anhang aufgeführt.

Nachfolgend werden die wichtigsten Erkenntnisse zusammenfassend berichtet und kommentiert.

Dr. Oliver Bruttel
Institut für Demoskopie Allensbach
Allensbach am Bodensee

Prof. Dr. Klaus Schweinsberg
Centrum für Strategie und Höhere Führung
Bodman am Bodensee

IT- und Datensicherheit als gesellschaftliche Risiken

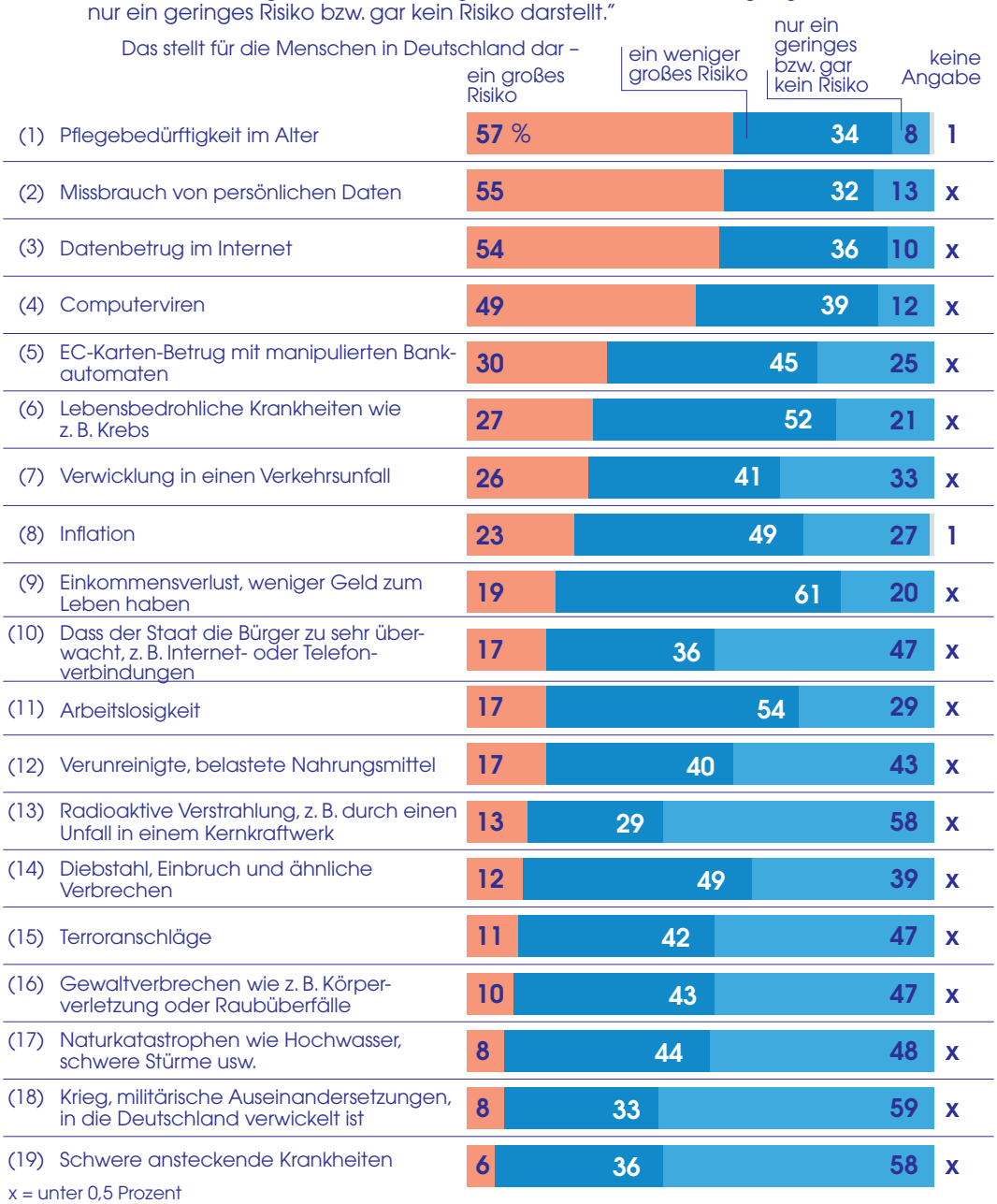
Nach Einschätzung der Entscheidungsträger aus Wirtschaft und Politik stellen Cybergefahren und Datenschutzverletzungen unter 19 Risiken aus allen Lebensbereichen mit das größte Risikopotenzial für die Bevölkerung in Deutschland dar. 55 Prozent sehen im Missbrauch persönlicher Daten ein großes Risiko für die Menschen in Deutschland, 54 Prozent im Datenbetrug im Internet, 49 Prozent in Computerviren. Mindestens eine der drei Gefahren erachten 77 Prozent der Entscheidungsträger als großes Risiko für die Bürger.

Im Vergleich zu den einzelnen IT- und Datenrisiken wird nur die Pflegebedürftigkeit im Alter vor dem Hintergrund des demografischen Wandels mit 57 Prozent als vergleichbar großes Risiko für die Bevölkerung eingestuft. Demgegenüber empfinden Abgeordnete und Führungskräfte aus der Wirtschaft Gefahrenquellen in anderen Lebensbereichen als deutlich weniger risikorelevant für die Gesellschaft. Am ehesten noch gilt der EC-Karten-Betrug mit manipulierten Bankautomaten, der im weitesten Sinn noch zu den Cybergefahren gezählt werden kann, mit 30 Prozent als großes Risiko. Lebensbedrohliche Krankheiten und die Verwicklung in einen Verkehrsunfall betrachten 27 bzw. 26 Prozent der Entscheidungsträger als großes Risiko für die Menschen. Materielle Risiken wie Inflation, Einkommensverlust oder Arbeitslosigkeit folgen mit 23, 19 bzw. 17 Prozent (Schaubild 1).

Schaubild 1

Die Risikowahrnehmung von Entscheidungsträgern aus Wirtschaft und Politik

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."



x = unter 0,5 Prozent

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft

Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Bemerkenswerterweise stufen die Entscheidungsträger aus Wirtschaft und Politik die Risiken für die Bevölkerung, die von Cyber- und Datenkriminalität ausgehen, – allerdings auf hohem Niveau – heute als geringer ein als vor einem Jahr. 2011 waren 64 Prozent der Entscheidungsträger der Meinung, dass vom Missbrauch persönlicher Daten eine große Gefahr für die Bevölkerung ausgehe, aktuell sind es 55 Prozent. Ein ähnliches Bild zeigt sich beim Datenbetrug im Internet, den vor einem Jahr 67 Prozent als großes Risiko einstuften, aktuell sind es 54 Prozent. Die Sicherheitsgefährdung, die von Computerviren ausgeht, wird mit 49 Prozent ebenfalls geringer eingestuft als im Vorjahr, als 59 Prozent der Entscheidungsträger darin ein großes gesellschaftliches Risiko sahen.

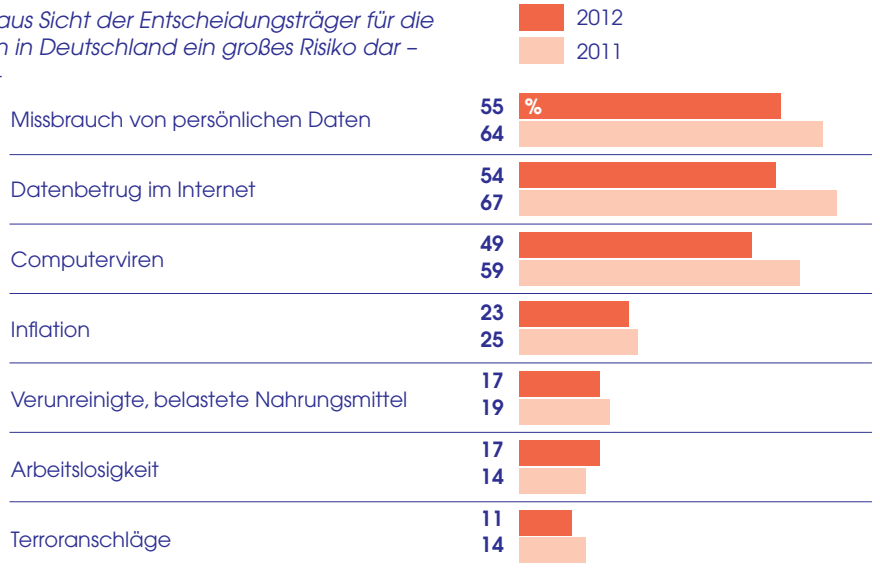
Bei anderen Risiken gab es dagegen keine signifikante Veränderung der Sicherheitseinschätzung. So bewertet aktuell wie auch vor einem Jahr rund ein Viertel der Entscheidungsträger die Inflation als großes Risiko für die Bevölkerung. Der Arbeitslosigkeit wird derzeit von 17 Prozent ein großes gesellschaftliches Risikopotenzial zugebilligt, 2011 waren es 14 Prozent (Schaubild 2).

Ein wesentlicher Grund für den deutlichen Rückgang bei der Bewertung von IT- und Datenrisiken dürfte sein, dass in den zurückliegenden zwölf Monaten andere Risiken – insbesondere in den Finanzmärkten – die tagespolitische Agenda und die Medienberichterstattung dominiert haben, was nicht ohne Folgen auf die Risikowahrnehmung blieb.

Schaubild 2

Auf hohem Niveau rückläufige Risikowahrnehmung von Cyber- und Datenrisiken bei den Entscheidungsträgern

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



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfragen 6220 (Juli 2011) und 6240 (Juni/Juli 2012)

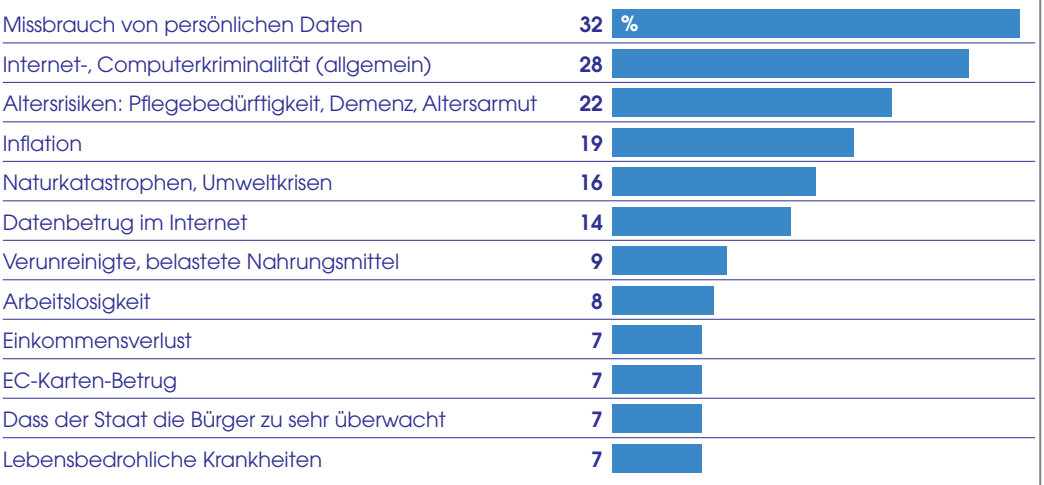
Als zukünftige Gefährdungsquellen messen Abgeordnete und Führungskräfte aus der Wirtschaft der Internet- und Computerkriminalität sowie dem Missbrauch persönlicher Daten im Vergleich zu anderen Risiken gleichwohl weiterhin die größte Bedeutung bei. Mit beachtlicher Deutlichkeit benennen die Entscheidungsträger aus Wirtschaft wie auch aus Politik Internet- und IT-Risiken ganz spontan als herausragende Zukunftsgefahren. 32 Prozent verweisen auf den Missbrauch persönlicher Daten als wachsende Gefahrenquelle, 28 Prozent auf Internet- und Computerkriminalität generell. 14 Prozent rechnen mit einer besonders starken Zunahme von Datenbetrug im Internet. 67 Prozent der Entscheidungsträger erwarten, dass mindestens eines der Risiken künftig stark zunehmen wird.

Unter den anderen Bereichen sehen die Entscheidungsträger – neben der Pflegebedürftigkeit im Alter mit 22 Prozent – insbesondere eine steigende Inflation sowie ein vermehrtes Auftreten von Naturkatastrophen als Risiko für Deutschland an. Rund jeder fünfte Entscheidungsträger nennt spontan die Geldentwertung als Risiko, das in Zukunft besonders zunehmen wird, 16 Prozent Naturkatastrophen und Umweltkrisen. Mit einer starken Zunahme anderer Risiken rechnen nur wenige Entscheidungsträger (Schaubild 3).

Schaubild 3

Risiken, die aus Sicht von Entscheidungsträgern in Zukunft 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 5 Prozent und mehr

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

IT-Sicherheit mit hohem Stellenwert in den Unternehmen

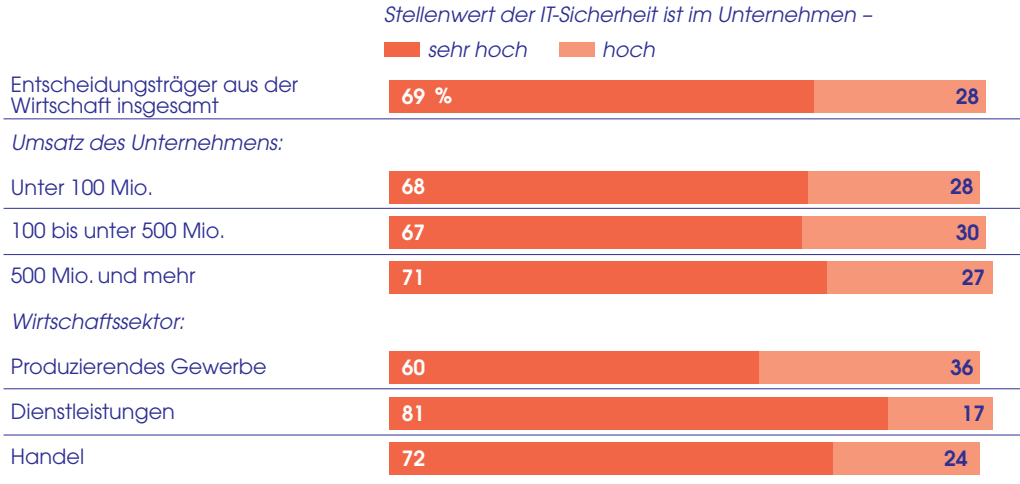
Mehr als zwei Drittel (69 Prozent) der Entscheidungsträger in der Wirtschaft messen dem Schutz des eigenen Unternehmensnetzwerks vor unerlaubten Zugriffen von außen einen sehr hohen, weitere 28 Prozent einen hohen Stellenwert bei.

Insbesondere im Dienstleistungs- und Handelssektor hat die IT-Sicherheit mit 81 bzw. 72 Prozent eine sehr hohe Relevanz (Schaubild 4).

Schaubild 4

IT-Sicherheit hat heute in allen größeren Unternehmen einen (sehr) hohen Stellenwert

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



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

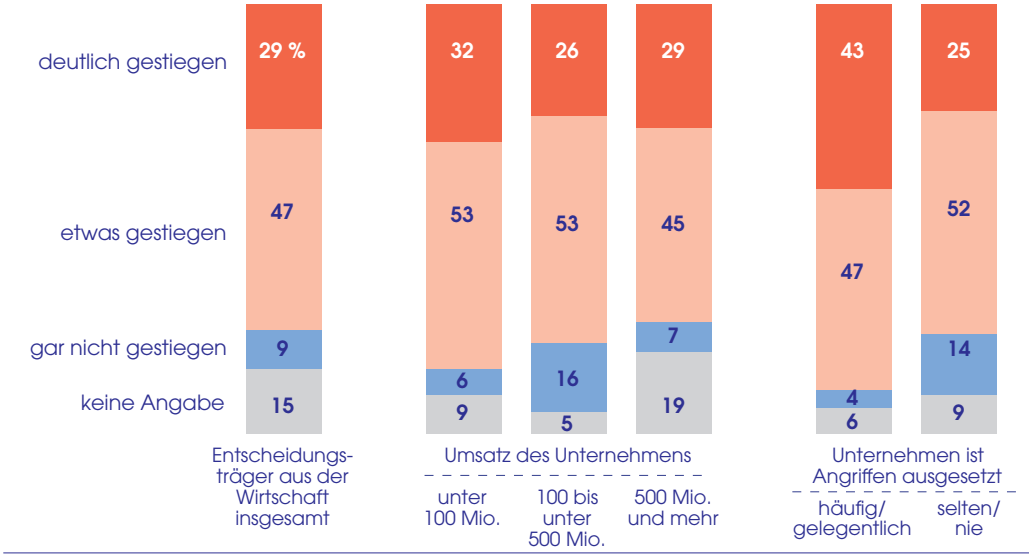
Mit dem hohen Stellenwert der IT-Sicherheit in Großunternehmen sind auch gestiegene Kosten verbunden: 29 Prozent der Entscheidungsträger aus der Wirtschaft sagen, dass sich ihre Kosten für IT-Sicherheit deutlich, 47 Prozent geben an, dass sie sich etwas erhöht haben.

Dabei ist für das Ausmaß des Kostenanstiegs weniger die Unternehmensgröße entscheidend als vielmehr die Frage, wie stark das Unternehmen Hacker-Angriffen ausgesetzt ist. In 43 Prozent der Unternehmen, die häufig oder gelegentlich mit solchen Angriffen auf ihr IT-System zu kämpfen haben, sind die Kosten für IT-Sicherheit in den letzten Jahren deutlich gestiegen. Von den Unternehmen, die nur selten oder sogar nie Hacker-Angriffe auf ihr Unternehmen wahrnehmen, verweist nur jedes vierte auf deutlich gestiegene Kosten (Schaubild 5).

Schaubild 5

Steigende Kosten für IT-Sicherheit

Frage: „Darf ich fragen, wie sich die Kosten für IT-Sicherheit, für den Schutz vor Hacker-Angriffen in den letzten Jahren bei Ihnen entwickelt haben? Sind die Kosten in diesem Bereich ..."



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

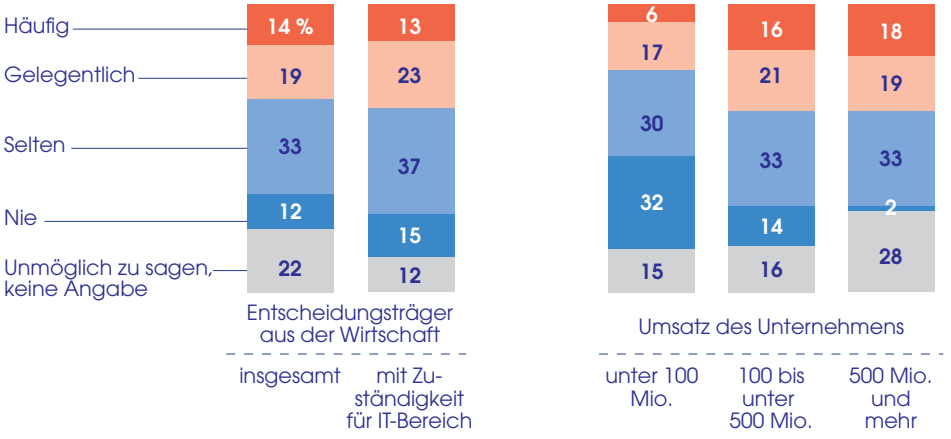
Zwei Drittel der deutschen Unternehmen berichten über IT-Angriffe von außen. 14 Prozent der Führungskräfte aus der Wirtschaft geben zu Protokoll, dass häufig, weitere 19 Prozent, dass gelegentlich versucht wird, ihr Unternehmen auszuspionieren oder zu schädigen. Bei jedem dritten Unternehmen gibt es zumindest selten Hacker-Angriffe auf das Unternehmensnetzwerk. Führungskräfte, die für den IT-Bereich in ihrem Unternehmen verantwortlich sind und damit unmittelbaren Einblick in die Gefährdungslage haben, äußern sich ähnlich: 73 Prozent nehmen IT-Angriffe auf ihr Unternehmen wahr, 36 Prozent konstatieren häufige oder gelegentliche Angriffe.

Die Häufigkeit der Angriffe hängt stark von der Größe des Unternehmens ab. Unternehmen mit einem Jahresumsatz von 500 Millionen Euro und mehr sind mit 18 Prozent dreimal mehr häufigen IT-Angriffen ausgesetzt als Unternehmen mit weniger als 100 Millionen Euro Umsatz, von denen nur 6 Prozent von häufigen Angriffen berichten (Schaubild 6).

Schaubild 6

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? Kommt das bei Ihnen häufig, gelegentlich, selten oder nie vor?"



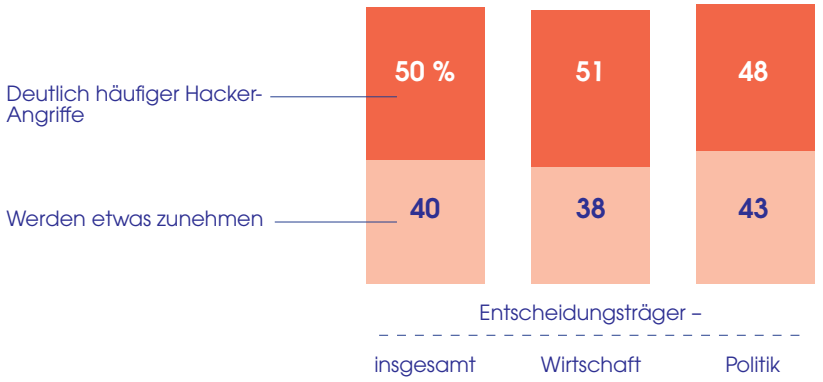
Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Neun von zehn Entscheidungsträgern rechnen künftig mit einer Zunahme von Hacker-Angriffen auf deutsche Behörden und Unternehmen. Jeweils rund die Hälfte der Führungskräfte aus der Wirtschaft und der Abgeordneten erwartet, dass solche Hacker-Angriffe deutlich zunehmen, 38 bzw. 43 Prozent gehen davon aus, dass solche Angriffe etwas zunehmen werden (Schaubild 7).

Schaubild 7

Mehrheit der Entscheidungsträger erwartet deutliche Zunahme der Hacker-Angriffe

Frage: „Wie sehen Sie das für die Zukunft: Wird es deutlich häufiger zu Hacker-Angriffen auf deutsche Behörden und Unternehmen kommen als zurzeit oder werden solche Hacker-Angriffe etwas zunehmen oder rechnen Sie gar nicht mit einem Anstieg?"



Auf 100 fehlende Prozent: kein Anstieg; unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Wie bei der Einschätzung der gesellschaftlichen Risiken ist auch bei der erwarteten Entwicklung der Hacker-Angriffe ein rückläufiges Risikobewusstsein der Entscheidungsträger zu beobachten. Im Vorjahr erwarteten noch 66 Prozent eine deutliche Zunahme von Hacker-Angriffen auf deutsche Behörden und Unternehmen, 28 Prozent zumindest einen leichten Anstieg. Insgesamt rechnen zwar auch in diesem Jahr ähnlich viele mit einem Anstieg, aber der Anteil derjenigen, die eine deutliche Erhöhung erwarten, ist sichtbar zurückgegangen (Tabelle 1).

Tabelle 1

	Entscheidungsträger insgesamt	
	2011	2012
	%	%
Es erwarten für die Zukunft –		
deutlich häufiger Hacker-Angriffe	66	50
werden etwas zunehmen	28	40
	94	90

Quelle: Allensbacher Archiv, IfD-Umfragen 6220 (Juli 2011) und 6240 (Juni/Juli 2012)

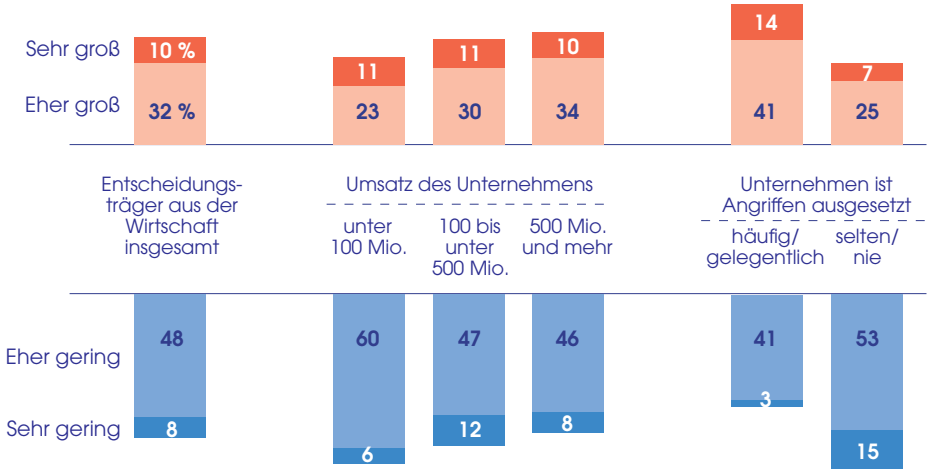
Die Mehrheit der Entscheidungsträger aus der Wirtschaft stuft das Risiko für das eigene Unternehmen, durch einen Hacker-Angriff gravierend geschädigt zu werden, als eher oder sehr gering ein. 32 Prozent sehen darin eine eher große, nur 10 Prozent eine sehr große Gefahr.

Die Unternehmensgröße hat dabei kaum einen Einfluss auf die Risikobewertung. Auch von den Führungskräften aus Unternehmen mit 500 Millionen Euro und mehr Umsatz stufen nur 44 Prozent das Risiko als sehr groß oder groß ein, von den Unternehmen mit einem Umsatz zwischen 100 und unter 500 Millionen Euro im Jahr sind es 41 Prozent, von den Unternehmen mit weniger als 100 Millionen Euro 34 Prozent (Schaubild 8).

Schaubild 8

Mehrheit der Unternehmen stuft das Risiko, durch einen Hacker-Angriff gravierend geschädigt zu werden, als (eher) gering ein

Frage: „Was glauben Sie: Wie groß ist das Risiko für Unternehmen, durch einen Hacker-Angriff gravierend geschädigt zu werden? Ist das Risiko sehr groß, eher groß, eher gering oder sehr gering?"



Auf 100 fehlende Prozent: keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Auf die offene Frage – also ohne Antwortvorgaben –, welche Sicherheitsvorkehrungen man im Unternehmen getroffen hat, um sich gegen Hacker-Angriffe zu schützen, nennen die Führungskräfte aus der Wirtschaft mit Abstand am häufigsten die Einrichtung von Firewalls. Diese Schutzvorrichtung wurde von der Hälfte der Führungskräfte angegeben.

Andere Maßnahmen wurden spontan deutlich seltener genannt. So verwiesen 16 Prozent auf allgemein hohe Schutzstandards gegen externe Zugriffe, 13 Prozent pauschal auf den Einsatz üblicher standardmäßiger Sicherheitsvorkehrungen. Antivirensoftware erwähnten 12 Prozent, eine anspruchsvolle Passwortverwaltung 11 Prozent, 9 Prozent die regelmäßige Aktualisierung von Programmen. 8 Prozent der Führungskräfte führten spontan die Durchführung von Sicherheitschecks, z. B. die Simulation von Hackerangriffen, als Sicherheitsmaßnahme an (Schaubild 9).

Schaubild 9

Spontan genannte Sicherheitsvorkehrungen zum Schutz vor Hacker-Angriffen

Frage: „Welche Sicherheitsvorkehrungen haben Sie in Ihrem Unternehmen getroffen, um sich vor Hacker-Angriffen zu schützen?“ (offene Ermittlung, ohne Antwortvorgaben)

Nur Nennungen mit 5 Prozent und mehr

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Das Cloud Computing, also die Möglichkeit, eigene Daten und Programme extern im Internet statt auf dem eigenen Computer oder Firmenserver zu speichern, stößt bei den Entscheidungsträgern auf erhebliche Sicherheitsbedenken.

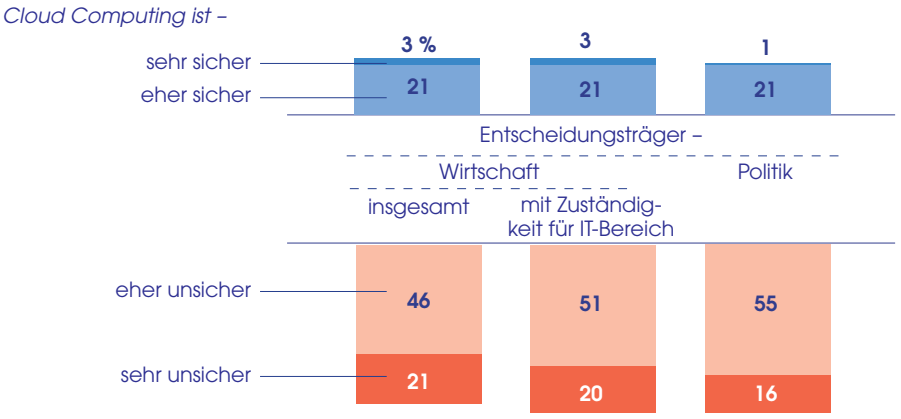
Von den Entscheidungsträgern in der Wirtschaft halten diese Art der Datenverarbeitung nur 3 Prozent für sehr sicher, 21 Prozent für eher sicher. Die überwiegende Mehrheit erachtet das Cloud Computing dagegen als eher unsicher (46 Prozent) oder sehr unsicher (21 Prozent).

Auch Führungskräfte, die in ihrem Unternehmen für den IT-Bereich verantwortlich sind, sehen das Cloud Computing kritisch. Bei den politischen Entscheidungsträgern stößt das Cloud Computing ebenfalls auf Skepsis (Schaubild 10).

Schaubild 10

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? Halten Sie das für ...“



Auf 100 fehlende Prozent: kommt darauf an, keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Trotz der zunehmenden Inanspruchnahme von Cloud Services durch Unternehmen wie auch Privatpersonen hat sich die kritische Einschätzung der Entscheidungsträger im Vergleich zum Vorjahr kaum verändert. Der Anteil derjenigen, die das Cloud Computing für sicher halten, liegt mit 23 Prozent kaum über dem Niveau von 2011, als 21 Prozent der Entscheidungsträger diese IT-Lösung als sicher einstuften (Tabelle 2).

Tabelle 2

	Entscheidungsträger insgesamt	
	2011	2012
	%	%
Cloud Computing ist –		
sehr sicher	2	2
eher sicher	19	21
eher unsicher	47	49
sehr unsicher	26	19

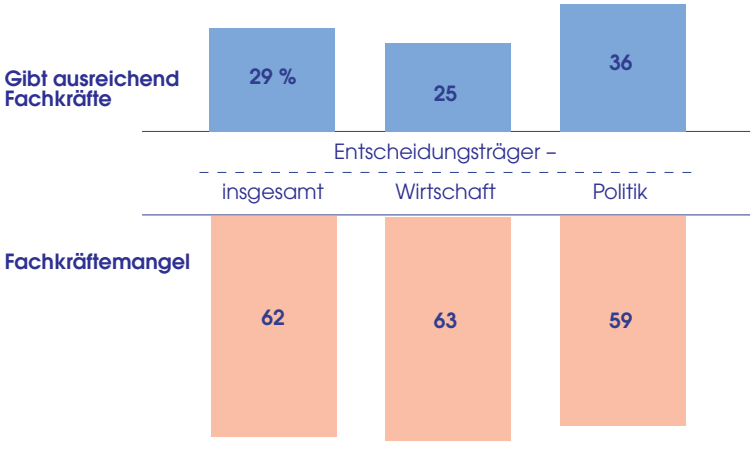
Auf 100 fehlende Prozent: kommt darauf an, keine Angabe
Quelle: Allensbacher Archiv, IfD-Umfragen 6220 (Juli 2011) und 6240 (Juni/Juli 2012)

Für die Umsetzung einer hohen IT-Sicherheit im Unternehmen ist die Verfügbarkeit gut ausgebildeter Fachkräfte eine wichtige Voraussetzung. Allerdings vermuten 62 Prozent der Entscheidungsträger einen Fachkräftemangel für den Bereich der IT-Sicherheit – von den Führungskräften in Unternehmen sind es 63 Prozent, von den Abgeordneten 59 Prozent, die hier von einem Engpass ausgehen (Schaubild 11).

Schaubild 11

Fachkräftemangel im Bereich IT-Sicherheit

Frage: „Gibt es in Deutschland ausreichend Fachkräfte für den Bereich IT-Sicherheit oder gibt es in diesem Bereich eher einen Fachkräftemangel?"



Auf 100 fehlende Prozent: schwer zu sagen, keine Angabe

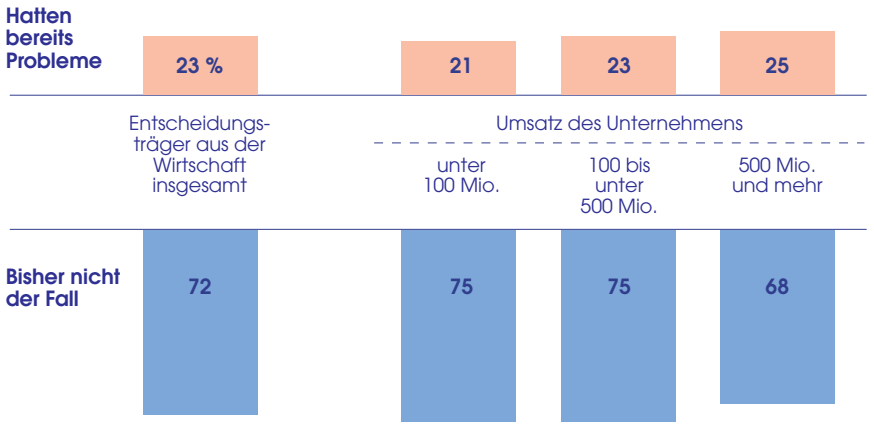
Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Bezogen auf das eigene Unternehmen, berichten allerdings nur 23 Prozent der Führungskräfte über Probleme, geeignete IT-Spezialisten für Sicherheitsfragen zu finden. 72 Prozent hatten bislang keine Probleme bei der Personalrekrutierung in diesem Bereich. Die Erfahrungen sind dabei in allen Größenklassen von Unternehmen ähnlich (Schaubild 12).

Schaubild 12

Allerdings bislang kaum Probleme im eigenen Unternehmen

Frage: „Und hatten Sie in Ihrem Unternehmen bereits Probleme, geeignete IT-Spezialisten für Sicherheitsfragen zu finden, oder war das bisher nicht der Fall?"



Auf 100 fehlende Prozent: keine Angabe

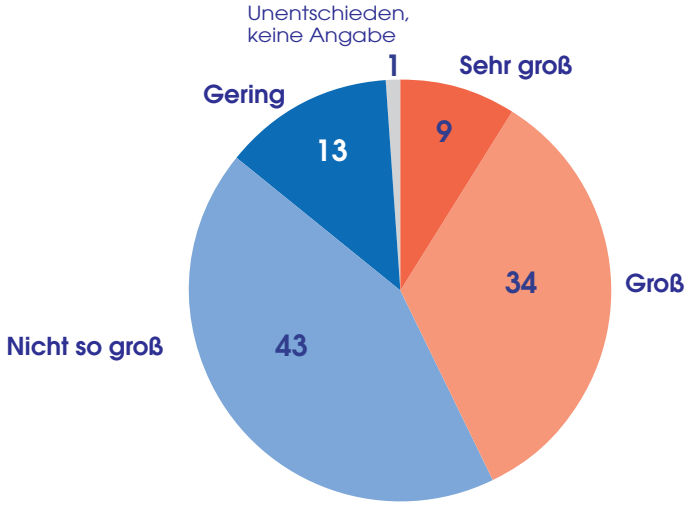
Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Neben der Bedrohung durch externe IT-Angriffe kann die unberechtigte Weitergabe sensibler Daten von Mitarbeitern an Dritte ein Sicherheitsrisiko für Unternehmen sein. 9 Prozent der Führungskräfte aus der Wirtschaft halten diese Gefahr für sehr groß, 34 Prozent für groß. 56 Prozent bewerten das Risiko dagegen als weniger groß oder gering (Schaubild 13).

Schaubild 13

Einschätzung der Gefahr, dass durch Mitarbeiter sensible Daten nach außen gegeben werden

Frage: „Wie groß ist Ihrer Einschätzung nach in Ihrem Unternehmen die Gefahr, dass Mitarbeiter durch unberechtigte Weitergabe sensibler Daten nach außen Schaden verursachen?“



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Schutz vor Cyberkriminalität bleibt Herausforderung für die Politik

In der Bewertung, wieweit die Politik grundsätzlich angemessen mit den Risiken für die Menschen in Deutschland umgeht, unterscheiden sich die Einschätzungen von Abgeordneten und Führungskräften aus der Wirtschaft nach wie vor erheblich, die Unterschiede haben sich im Vergleich zum Vorjahr aber etwas verringert.

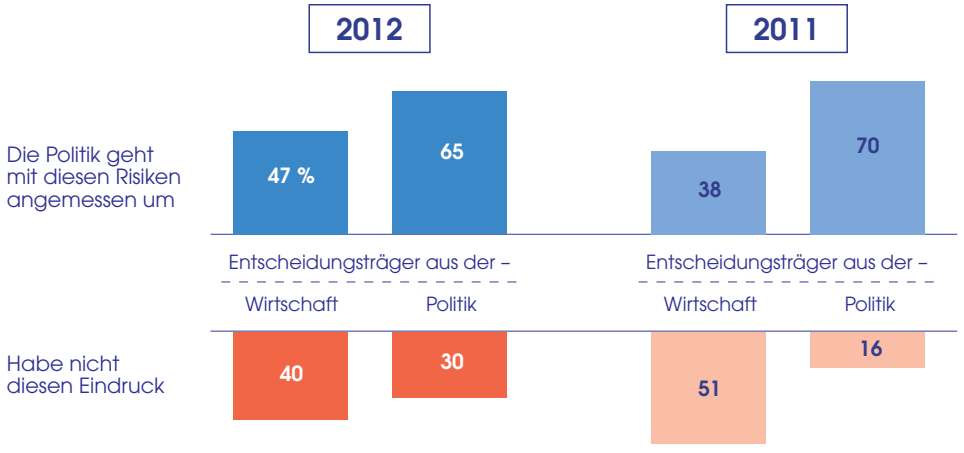
Aktuell sind 47 Prozent der Führungskräfte aus der Wirtschaft und 65 Prozent der Abgeordneten der Meinung, dass die Politik insgesamt angemessen mit den Risiken umgeht. 40 Prozent der Entscheidungsträger aus der Wirtschaft, 30 Prozent der Entscheidungsträger aus der Politik sehen das anders.

Damit hat sich das Stimmungsbild in der Wirtschaft im Vergleich zum Vorjahr gewandelt: Damals waren nur 38 Prozent der Entscheidungsträger aus der Wirtschaft von einem adäquaten Umgang der Politik mit den Risiken überzeugt, eine Mehrheit von 51 Prozent dagegen skeptisch (Schaubild 14).

Schaubild 14

Angemessener Umgang der Politik mit den Risiken?

Frage: „Wir haben ja gerade über verschiedene Risiken und somit über verschiedene Facetten von Sicherheit gesprochen. Einmal ganz allgemein gefragt: Haben Sie den Eindruck, dass die Politik alles in allem angemessen mit diesen Risiken für die Menschen in Deutschland umgeht, oder haben Sie nicht diesen Eindruck?“



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfragen 6220 (Juli 2011) und 6240 (Juni/Juli 2012)

Bei den spontan – also ohne die Vorgabe möglicher Antwortalternativen – genannten Bereichen, in denen die Politik aus Sicht der Entscheidungsträger aktiv werden sollte, stehen wie im Vorjahr Datenschutz und Datensicherheit sowie der Kampf gegen die Internetkriminalität an oberster Stelle.

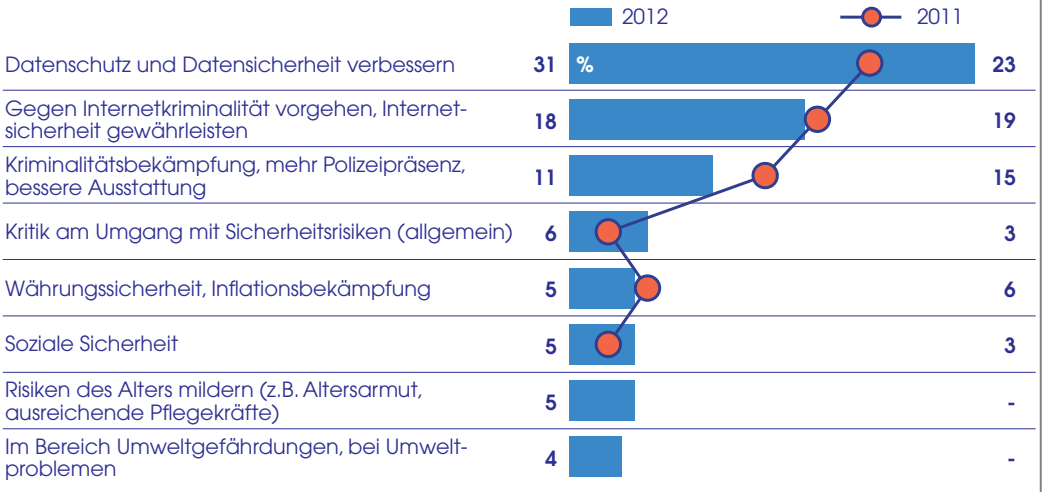
31 Prozent der Entscheidungsträger fordern eine aktivere Rolle der Politik bei der Verbesserung von Datenschutz und Datensicherheit, 18 Prozent bei der Gewährleistung von Sicherheit im Internet. 2011 waren es 23 bzw. 19 Prozent, die sich in den jeweiligen Bereichen mehr Einsatz seitens der Politik wünschten.

Von den anderen Politikbereichen spielt mit 11 Prozent am ehesten noch die „klassische" Kriminalitätsbekämpfung, z. B. durch mehr Polizeipräsenz oder eine bessere Ausstattung der Sicherheitsbehörden, eine Rolle. 6 Prozent äußern allgemeine Kritik am Umgang mit Sicherheitsrisiken. Zusätzliche Maßnahmen in anderen Sicherheitsbereichen werden – zumindest spontan – nur von 5 Prozent oder weniger der Entscheidungsträger genannt (Schaubild 15).

Schaubild 15

Wo die Politik aus Sicht der Entscheider aktiv werden sollte, um mehr Sicherheit zu gewährleisten

Frage: „Gibt es beim Thema Sicherheit Bereiche, in denen die Politik etwas verändern, in denen sie aktiv werden sollte?" (offene Ermittlung, ohne Antwortvorgaben)



2012: nur Nennungen mit 4 Prozent und mehr

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfragen 6220 (Juli 2011) und 6240 (Juni/Juli 2012)

Datenschutz und Datensicherheit ist dabei ein Thema, das besonders stark von Entscheidungsträgern aus der Wirtschaft genannt wird: 35 Prozent der Führungskräfte aus der Wirtschaft und 25 Prozent der Abgeordneten sehen darin einen Bereich, in dem die Politik stärker aktiv werden sollte.

Unter den anderen Sicherheitsbereichen ist insbesondere die soziale Sicherheit ein Thema, bei dem die Abgeordneten mit 9 Prozent einen größeren Handlungsbedarf sehen als die Führungskräfte aus der Wirtschaft, von denen nur 3 Prozent spontan der Auffassung sind, dass die Politik hier stärker aktiv werden sollte (Tabelle 3).

Tabelle 3

	Entscheidungsträger –	
	Wirtschaft	Politik
	%	%
Da sollte die Politik aktiver werden –		
Datenschutz und Datensicherheit verbessern	35	25
Gegen Internetkriminalität vorgehen	18	18
Kriminalitätsbekämpfung allgemein	13	9
Allgemein: Kritik am Umgang mit Sicherheitsrisiken	5	7
Währungssicherheit, Inflationsbekämpfung	7	2
Soziale Sicherheit	3	9
Risiken des Alters mildern	4	6
Im Bereich Umweltgefährdungen, bei Umweltproblemen	4	5

Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Um angemessen auf Risiken reagieren zu können, bedarf es bei Gesetzgeber wie auch Verwaltung ausreichender Fachkompetenz, um Risiken einschätzen, adäquate Handlungsstrategien ableiten und diese auch effektiv umsetzen zu können. Die Entscheidungsträger bewerten diese Fachkompetenz von Politik und Verwaltung je nach Sicherheitsbereich sehr unterschiedlich.

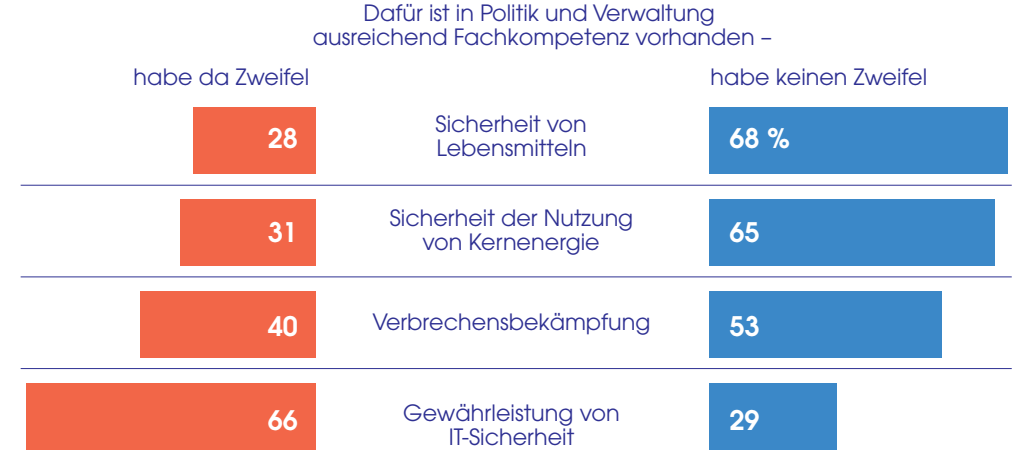
Besonders hohe Fachkompetenz wird Legislative und Exekutive für den Bereich der Lebensmittelsicherheit und der sicheren Nutzung der Kernenergie zugeschrieben. In beiden Bereichen zeigen sich rund zwei Drittel der Entscheidungsträger davon überzeugt, dass ausreichend Fachkompetenz vorhanden ist. Nur 28 bzw. 31 Prozent zweifeln in diesen Sachgebieten an den Fähigkeiten von Politik und Verwaltung. Auch bei der Verbrechensbekämpfung überwiegt mit 53 Prozent die positive Bewertung der Kompetenz von Politik und Verwaltung.

Ganz anders dagegen bei der Gewährleistung von IT-Sicherheit: Nur 29 Prozent können hier ausreichende Fachkompetenz bei Politik und Behörden erkennen, zwei Drittel haben Zweifel (Schaubild 16).

Schaubild 16

Einschätzung der Fachkompetenz von Politik und Verwaltung

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



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

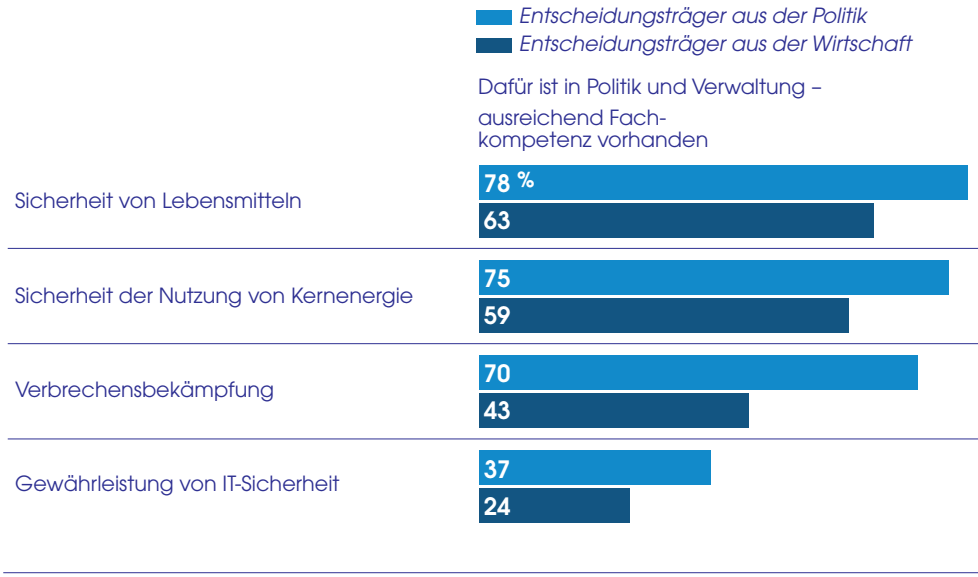
Generell bewerten die Entscheidungsträger aus der Wirtschaft die Kompetenz von Politik und Verwaltung kritischer als die befragten Abgeordneten. So halten 78 Prozent der Abgeordneten die Fachkompetenz von Regierung, Parlamenten und Behörden im Bereich der Lebensmittelsicherheit für ausreichend, von den Führungskräften aus der Wirtschaft liegt der Wert bei 63 Prozent. Ähnlich viele sind es bei der Nutzung der Kernenergie.

Bei der Verbrechensbekämpfung ist es mit 43 Prozent nur eine Minderheit der Führungskräfte aus der Wirtschaft, die den staatlichen Funktionsträgern ausreichende Fachkompetenz bei der inneren Sicherheit attestiert. Dagegen zeigt sich mit 70 Prozent die deutliche Mehrheit der Abgeordneten von der Fachkompetenz staatlicher Stellen auf diesem Gebiet überzeugt.

Bei der Gewährleistung von IT-Sicherheit schließlich gibt es nicht nur bei den Führungskräften aus der Wirtschaft, sondern auch bei den Abgeordneten erhebliche Zweifel an der vorhandenen Fachkompetenz. Nur 37 Prozent der Abgeordneten und 24 Prozent der Führungskräfte aus der Wirtschaft glauben, dass für diesen Bereich angemessenes Know-how in Politik und Verwaltung vorhanden ist (Schaubild 17).

Schaubild 17

Entscheidungsträger aus der Wirtschaft zweifeln stärker an der Fachkompetenz von Politik und Verwaltung, vor allem bei der IT-Sicherheit und Verbrechensbekämpfung



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

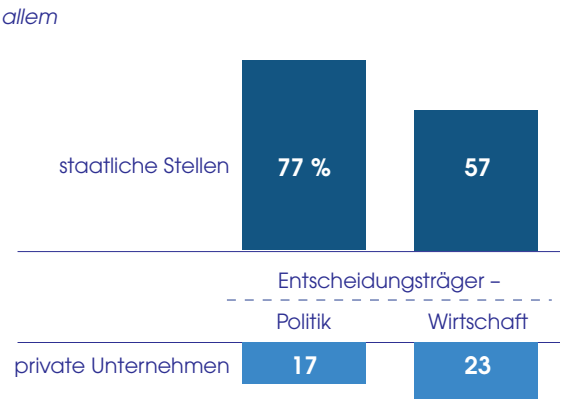
Im Bereich der Gewährleistung von IT-Sicherheit wird künftig insbesondere die Sicherung der Funktionsfähigkeit von Kommunikations- und Datenübertragungsnetzen an Bedeutung gewinnen. Sicherheitsstudien verweisen immer wieder auf die Gefahr eines Cyberkriegs, der in Form eines Angriffs auf kritische Infrastrukturen in Deutschland stattfinden kann.

In Bezug auf die Aufrechterhaltung der Kommunikations- und Datenübertragungsnetze sehen die Entscheidungsträger überwiegend den Staat in der Hauptverantwortung. So plädieren 77 Prozent der Abgeordneten und 65 Prozent der Führungskräfte aus der Wirtschaft für eine primäre Zuständigkeit staatlicher Stellen, wenn es darum geht, die Funktionsfähigkeit der Kommunikations- und Datenübertragungsnetze in Deutschland sicherzustellen. Nur eine Minderheit sieht hier die primäre Verantwortung bei privaten Unternehmen (Schaubild 18).

Schaubild 18

Zuständigkeit für die Sicherung der Funktionsfähigkeit der Kommunikations- und Datenübertragungsnetze

Frage: „Wer sollte Ihrer Meinung nach in erster Linie dafür zuständig sein, die Funktionsfähigkeit der Kommunikations- und Datenübertragungsnetze in Deutschland sicherzustellen und gegen Cyberangriffe zu verteidigen: staatliche Stellen oder private Unternehmen?"



Auf 100 fehlende Prozent: weder noch; unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Unternehmen wie Google oder Facebook als Handlungsfeld für die Politik

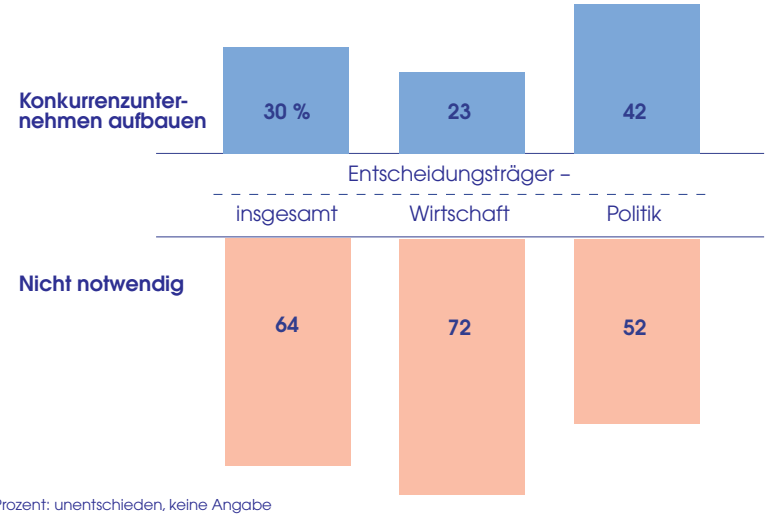
In vielen Bereichen des Internets oder digitaler Medien dominieren US-amerikanische Unternehmen wie Google, Facebook oder Apple derzeit den Markt. Aus Sicht der Entscheidungsträger besteht hier allerdings kein Bedarf, durch gezielte Industriepolitik ein europäisches Gegengewicht zu schaffen.

Nur 30 Prozent der Entscheidungsträger sind der Ansicht, dass sich Europa darum bemühen sollte, entsprechende Konkurrenzunternehmen aufzubauen, 64 Prozent sehen dazu keine Notwendigkeit. Unter den Führungskräften aus der Wirtschaft ist der Zuspruch noch geringer: Dort sehen nur 23 Prozent einen Bedarf, von den Abgeordneten sind es immerhin 42 Prozent (Schaubild 19).

Schaubild 19

Keine Notwendigkeit zum Aufbau europäischer Konkurrenzunternehmen zu Google, Facebook oder Apple

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



Auf 100 fehlende Prozent: unentschieden, keine Angabe

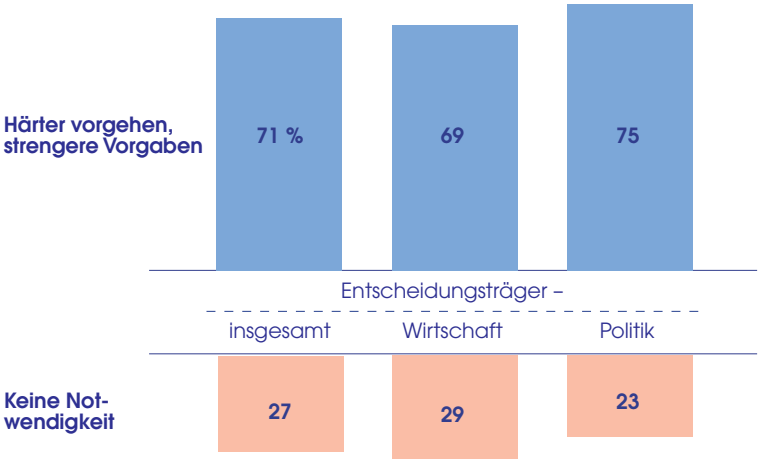
Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Gleichwohl vertritt eine Mehrheit der Entscheidungsträger aus Wirtschaft und Politik die Auffassung, dass Unternehmen wie Google, Facebook oder Apple durch strengere Vorgaben daran gehindert werden sollten, zu viele persönliche Daten ihrer Nutzer zu sammeln. 75 Prozent der Abgeordneten und 69 Prozent der Führungskräfte aus der Wirtschaft wünschen sich ein härteres Vorgehen. 23 Prozent der Abgeordneten sowie 29 Prozent der Führungskräfte aus der Wirtschaft sehen hierzu keine Notwendigkeit (Schaubild 20).

Schaubild 20

Strengere Vorgaben für Unternehmen, die persönliche Daten ihrer Nutzer sammeln

Frage: „Unternehmen wie Google, Facebook oder Apple wird ja immer wieder vorgeworfen, zu viele persönliche Daten ihrer Nutzer zu sammeln. Sind Sie der Meinung, dass man dagegen härter vorgehen müsste, z. B. durch strengere Vorgaben, welche Daten gesammelt bzw. gespeichert werden dürfen, oder sehen Sie dafür keine Notwendigkeit?"



Auf 100 fehlende Prozent: unentschieden, keine Angabe

Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

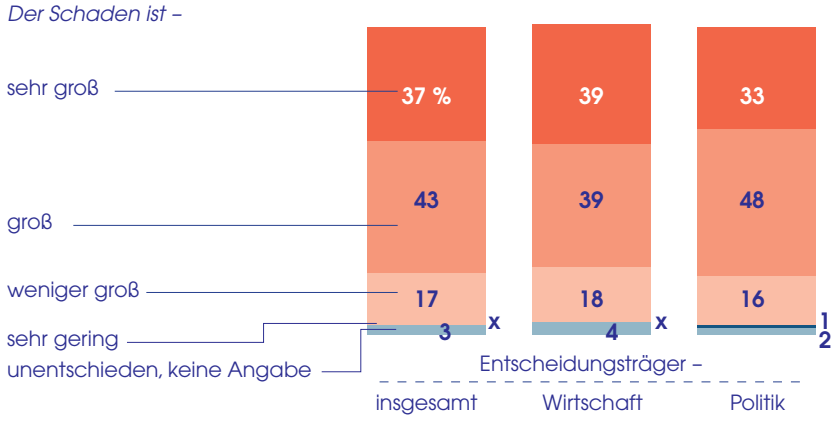
Wirtschafts- und Industriespionage

Eine spezifische Facette der IT-Sicherheit bildet die Wirtschafts- und Industriespionage. Mit rund 80 Prozent hält die überwältigende Mehrheit der Entscheidungsträger sowohl aus der Wirtschaft als auch der Politik den Schaden, welcher der deutschen Wirtschaft durch Industriespionage entsteht, für groß oder sehr groß. Nur 18 Prozent der Führungskräfte aus der Wirtschaft und 17 Prozent der Abgeordneten stufen den Schaden als weniger groß oder sehr gering ein (Schaubild 21).

Schaubild 21

Hoher Schaden durch Wirtschafts- und Industriespionage

Frage: „Zum Thema Wirtschafts- und Industriespionage: Wie groß ist Ihrer Einschätzung nach der Schaden für die deutsche Wirtschaft, der jedes Jahr durch Industriespionage entsteht?"



x = weniger als 0,5 Prozent

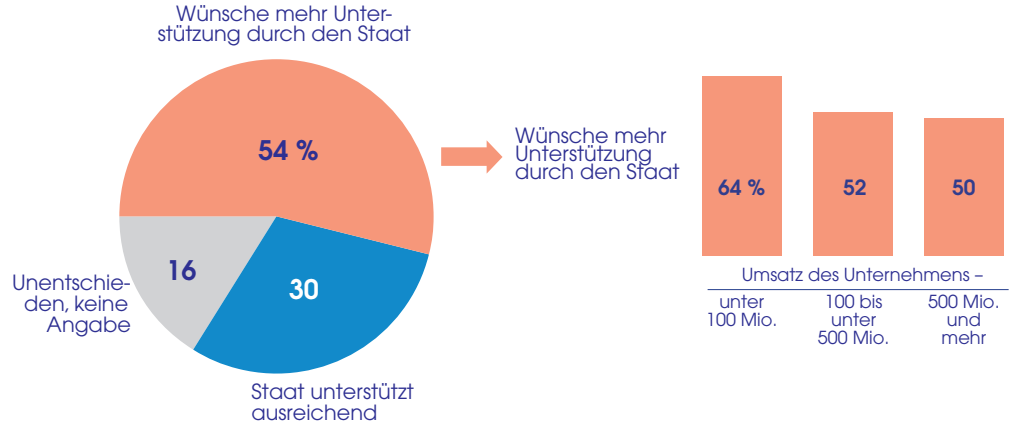
Basis: Bundesrepublik Deutschland, Entscheidungsträger aus Politik und Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Die Mehrheit der Unternehmen fühlt sich beim Thema Industriespionage von der Politik nicht ausreichend unterstützt. Gut jede zweite Führungskraft aus der Wirtschaft fordert mehr Unterstützung durch den Staat bei der Bekämpfung der Industriespionage. Selbst von den Führungskräften der besonders großen Unternehmen mit mehr als 500 Millionen Euro Umsatz erwarten 50 Prozent hierbei mehr staatliche Unterstützung, von den Unternehmen mit weniger als 100 Millionen Euro Umsatz sind es 64 Prozent (Schaubild 22).

Schaubild 22

Mehr Unterstützung durch den Staat bei der Bekämpfung von Industriespionage

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



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Die Führungskräfte aus der Wirtschaft erachten vor allem die stärkere internationale Zusammenarbeit auf politischer Ebene als geeignete Maßnahme von staatlicher Seite, um die Industriespionage gegen deutsche Unternehmen einzudämmen. 58 Prozent bewerten das als sehr hilfreich, 29 Prozent als hilfreich.

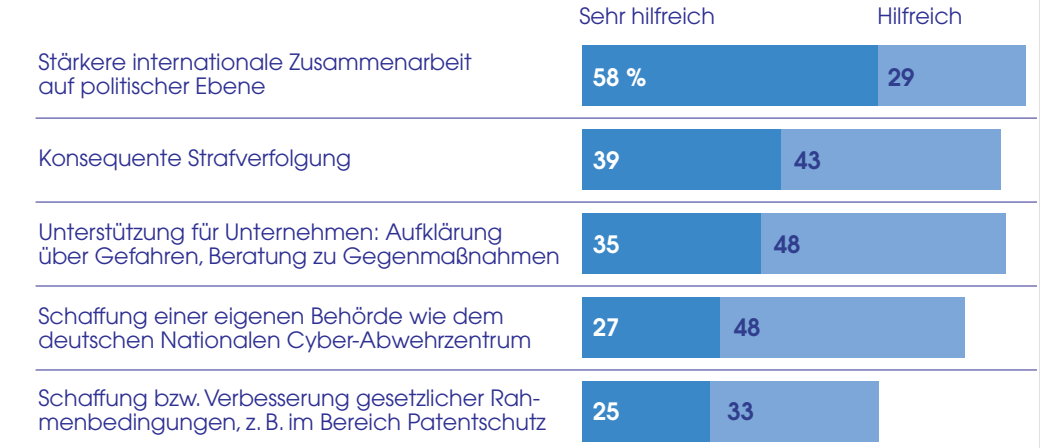
Darüber hinaus gilt die konsequente Strafverfolgung, auch in Form härterer Strafen für die Täter bzw. Sanktionen gegen Länder, die Industriespionage betreiben, als besonders effektives Mittel. 35 Prozent halten die konkrete staatliche Unterstützung von Unternehmen, z. B. in Form von stärkerer Aufklärungsarbeit sowie Beratung zu Gegenmaßnahmen für sehr hilfreich.

Als vergleichsweise gering wird der Beitrag einer eigenen Behörde wie des deutschen Nationalen Cyber-Abwehrzentrums zur Eindämmung der Industriespionage gegen deutsche Unternehmen eingestuft. Nur 27 Prozent betrachten diese Maßnahme als sehr hilfreich. Die Verbesserung des Patentschutzes bewerten 25 Prozent als besonders effektiv (Schaubild 23).

Schaubild 23

Geeignete staatliche Maßnahmen zur Eindämmung der Industriespionage

Frage: „Was sind Ihrer Meinung nach geeignete Maßnahmen des Staates, um die Industriespionage gegen deutsche Unternehmen einzudämmen?"



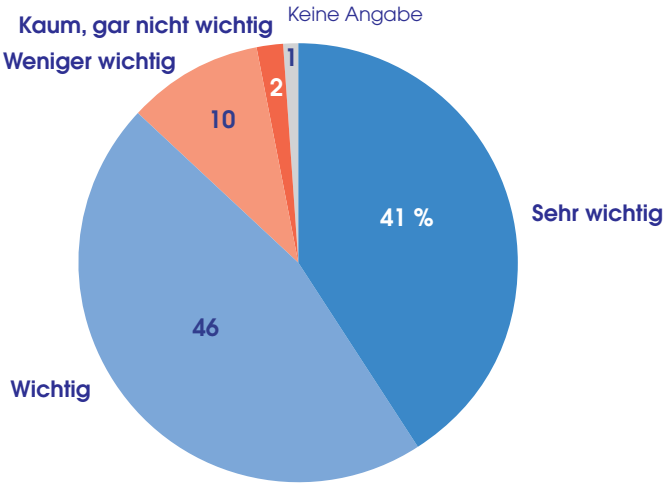
Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Neben staatlichen Maßnahmen ist aus Sicht der Entscheidungsträger aus der Wirtschaft aber auch der stärkere Austausch zwischen deutschen Unternehmen selbst wichtig, um der Industriespionage besser vorbeugen zu können. 41 Prozent halten den Dialog untereinander für sehr wichtig, 46 Prozent für wichtig (Schaubild 24).

Schaubild 24

Stärkerer Austausch zwischen Unternehmen zur Vorbeugung gegen Industriespionage

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



Basis: Bundesrepublik Deutschland, Entscheidungsträger aus der Wirtschaft
Quelle: Allensbacher Archiv, IfD-Umfrage 6240 (Juni/Juli 2012)

Studiendesign im Überblick

Repräsentative Befragung von Entscheidungsträgern aus Wirtschaft und Politik

Stichprobe:

a) 128 Abgeordnete, davon
44 Bundestagsabgeordnete,
70 Landtagsabgeordnete und
14 deutsche Abgeordnete im EU-Parlament

b) 214 Führungskräfte aus großen Unternehmen, davon
110 Inhaber, Geschäftsführer oder Vorstände und
104 andere Führungskräfte (z. B. Bereichsleiter)

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

Methode: telefonische Interviews

Befragungszeitraum: 5. Juni bis 9. Juli 2012