Deloitte.

Cyber Security Report 2021

Wahljahr 2021 – digitale Meinungsbildung ein Risiko

MAKING AN IMPACT THAT MATTERS since 1845

Vorwort

Erstmalig in Deutschland hat der Landkreis Anhalt-Bitterfeld in Sachsen-Anhalt im Juli 2021 den Cyber-Katastrophenfall ausgerufen. Nach einem Hacker-Angriff auf das Computersystem musste die Verwaltung ihre Arbeit für zwei Wochen einstellen und konnte vorerst keine Sozial- und Unterhaltsleistungen mehr auszahlen. Auf globaler Ebene waren auch die Nachwirkungen eines Cyber-Angriffs auf den US-amerikanischen IT-Dienstleister Kaseya im Sommer 2021 in Deutschland zu spüren. Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) gingen Meldungen von betroffenen Unternehmen ein, deren Dienstleistungen und Kunden durch den Angriff in Mitleidenschaft gezogen worden seien.

Diese Beispiele unterstreichen nicht nur die grenzüberschreitende Notwendigkeit von Cyber-Sicherheit, sondern zeigen klar die potenziellen Auswirkungen auf kommunaler, nationaler und internationaler Ebene auf.

Gemeinsam mit dem Institut für Demoskopie Allensbach hat Deloitte zum zehnten Mal eine repräsentative Trendstudie durchgeführt, um den Stand der Cyber-Sicherheit in Deutschland zu erheben. Befragt wurden 404 Führungskräfte aus Unternehmen sowie 104 Abgeordnete aus den Landtagen, dem Bundestag sowie dem Europaparlament.

Somit generiert die Studie einzigartige Einblicke in die Einschätzung von Cyber-Risiken durch politische Abgeordnete, die maßgeblich in entsprechende Gesetzgebungsprozesse involviert sind. Darüber hinaus wird die Meinung von Entscheidungsträgern aus der Wirtschaft eingebunden, die entsprechende Budgets in den Unternehmen verwalten und Investitionsentscheidungen treffen.

Neben einer Auswertung der Top-Risiken werden in der vorliegenden Studie auch die Cyber-Sicherheit als breitere gesellschaftliche Verantwortung, die Stärkung technologischer Unabhängigkeit sowie die Zusammenarbeit von Politik und Wirtschaft thematisiert. Ebenso werden aktuelle und künftige Handlungsfelder aufgezeigt.

Adäquate Cyber-Sicherheitsmaßnahmen müssen diese und weitere Punkte berücksichtigen, um Vertraulichkeit, Verfügbarkeit und Integrität von Systemen und Prozessen zu gewährleisten. Nur so können allumfassende und vorausschauende Cyber-Sicherheitsstrategien entwickelt und umgesetzt werden.

Bei diesen und anderen Herausforderungen begleiten wir von Deloitte unsere Kunden im Rahmen von Cyber-Sicherheitsprojekten bereits seit vielen Jahren.

Der Ergebnisse des vorliegenden Berichtes sowie die daraus entwickelten Handlungsfelder basieren auf den Meinungen der Befragten. Die Inhalte spiegeln nicht in ihrer Gänze die Meinung von Deloitte wider.

In diesem Bericht wird aus Gründen der besseren Lesbarkeit teilweise das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

Vorwort 02
Executive Summary 04
Einschätzung der Gefährdung 06
Risiken durch soziale Medien 10
Herausforderungen durch die Corona-Pandemie 16
Schlüsseltechnologien für Cyber-Sicherheit 20
Zusammenarbeit von Politik und Wirtschaft 21
Mangelnder Informationsaustausch 21
Staatliche Maßnahmen 24
Mögliche Handlungsfelder 27
Ansprechpartner 30

Executive Summary

Wie bereits in vergangenen Untersuchungen festgestellt, werden unterschiedlichste Cyber-Risiken von jeweils deutlichen Mehrheiten der Entscheidungsträger in Wirtschaft und Politik als großes Risiko für die Menschen in Deutschland eingestuft. Im Vergleich zu vorherigen Erhebungen verbleiben die Einschätzungen vieler Cyber-Risiken auf hohem Niveau. Im Allgemeinen gibt es kaum, jedoch im Speziellen bemerkenswerte Unterschiede in den Einschätzungen von Abgeordneten und Wirtschaftsführern.

Datenbetrug im Internet ist höchstes Risiko

77 Prozent der Entscheidungsträger stufen die Gefahr durch Datenbetrug im Internet als hohes Risiko ein. Damit wird dieses vor den Gefahren durch Computerviren beziehungsweise Schadsoftware (76 Prozent) und Fake News (75 Prozent) als größtes Cyber-Risiko für die Menschen in Deutschland in diesem Jahr angesehen. Mit dieser Risikoeinstufung liegt die Gefahr durch Datenbetrug seit 2013 konstant unter den Top-3-Risiken aus Sicht der Entscheidungsträger.

Risiken von Social-Media-Plattformen als Gefahr für die Demokratie

Obwohl eine Mehrheit der Entscheidungsträger eher Chancen als Risiken durch soziale Medien für ihr(e) Unternehmen, Partei oder eigene Person sehen, hält insbesondere eine Mehrheit der Abgeordneten die politische Meinungsbildung durch den Einfluss sozialer Medien für gefährdet. Phänomene wie Fake News, Filterblasen und Shitstorms beeinträchtigen die Informationsaufnahme von Nutzern, lähmen konstruktive sowie respektvolle politische Debatten und gefährden damit unsere Demokratie.

Zunehmende Bedeutung von Cyber-Sicherheit durch Corona-Pandemie

Durch die Corona-Pandemie ist die Bedeutung der Cyber-Sicherheit verstärkt in den Fokus der Öffentlichkeit gelangt. Die Verbreitung der Homeoffice-Arbeit und die starke Vernetzung erhöhen die Angriffsfläche für Cyber-Kriminelle. Um dieser Herausforderung zu begegnen, hat ein Großteil der Entscheidungsträger spezielle IT-Sicherheitsmaßnahmen getroffen. Auch wenn das Risiko, das von Mitarbeitenden im Homeoffice ausgeht, insgesamt als eher gering eingeschätzt wird, bestehen bei einem Teil der Befragten Zweifel am Risikobewusstsein ihrer Mitarbeiter.

Schlüsseltechnologien als Treiber der Wettbewerbsfähigkeit

Die große Mehrheit der Abgeordneten und der Wirtschaftsführer erachtet es für die Cyber-Sicherheit in Deutschland als notwendig, dass wichtige Schlüsseltechnologien für die Digitalisierung und Vernetzung von deutschen oder europäischen Unternehmen hergestellt werden. Die Abhängigkeit von anderen Ländern im Bereich von Schlüsseltechnologien wird sehr kritisch gesehen.

„Der Druck auf Unternehmen und Politik, Cyber-Sicherheit in Führungspositionen zu priorisieren, wächst – auf der nationalen wie auf der internationalen Ebene. Aufsichtsräte, Unternehmens- und Behördenleitungen spielen eine Schlüsselrolle und stehen in der Verantwortung."

Prof. Dr. Renate Köcher | Geschäftsführung, Institut für Demoskopie Allensbach

Unzureichender Austausch zwischen Staat und Wirtschaft

Auch wenn eine gute Zusammenarbeit zwischen Politik und Wirtschaft essenziell für das Cyber-Sicherheitsniveau in Deutschland und Europa ist, wird der Austausch zwischen den beiden Seiten von knapp 80 Prozent der Entscheidungsträger als nicht ausreichend empfunden. Bedingt wird diese Wahrnehmung durch die Auffassung beider Seiten, dass Abgeordnete nicht gut über die Bedürfnisse der Wirtschaft informiert sind.

Einschätzung der Gefährdung

Datenbetrug im Internet stellt für 77 Prozent der Entscheidungsträger in diesem Jahr das größte Cyber-Risiko für die Menschen in Deutschland dar. In den vergangenen Jahren lag die Einschätzung bei 70 Prozent (2019), 68 Prozent (2017), 67 Prozent (2015) beziehungsweise 62 Prozent (2013) und stieg somit nicht nur auf einen Höchstwert an, sondern befindet sich seit Umfragebeginn im Jahr 2013 auch konstant unter den Top-3-Risiken aus Sicht der Entscheidungsträger. Auf Platz zwei der größten Cyber-Risiken in diesem Jahr folgen Computerviren beziehungsweise Schadsoftware mit 76 Prozent. Damit steigt die Einschätzung im Vergleich zu 2019 um elf Prozentpunkte an und verglichen mit 2013 sogar um 19 Prozentpunkte. Führten Fake News 2019 die Gefahrenliste mit 74 Prozent noch an, sehen 2021 zwar 75 Prozent der Entscheidungsträger ein hohes Risiko für die Menschen in Deutschland, was jedoch nur für Platz drei auf der diesjährigen Rangliste reicht.

„Das hohe Gefahrenpotenzial und die Vielfältigkeit von Cyber-Risiken nehmen weiter zu. Die Politik muss beim Management dieser Risiken proaktiv agieren und Akteure aus der Wirtschaft, Forschung und Gesellschaft einbinden."

Peter Wirnsperger | Lead Civil Government, Deloitte

Abb. 1 – Die größten Cyber-Risiken für die Menschen in Deutschland 2021

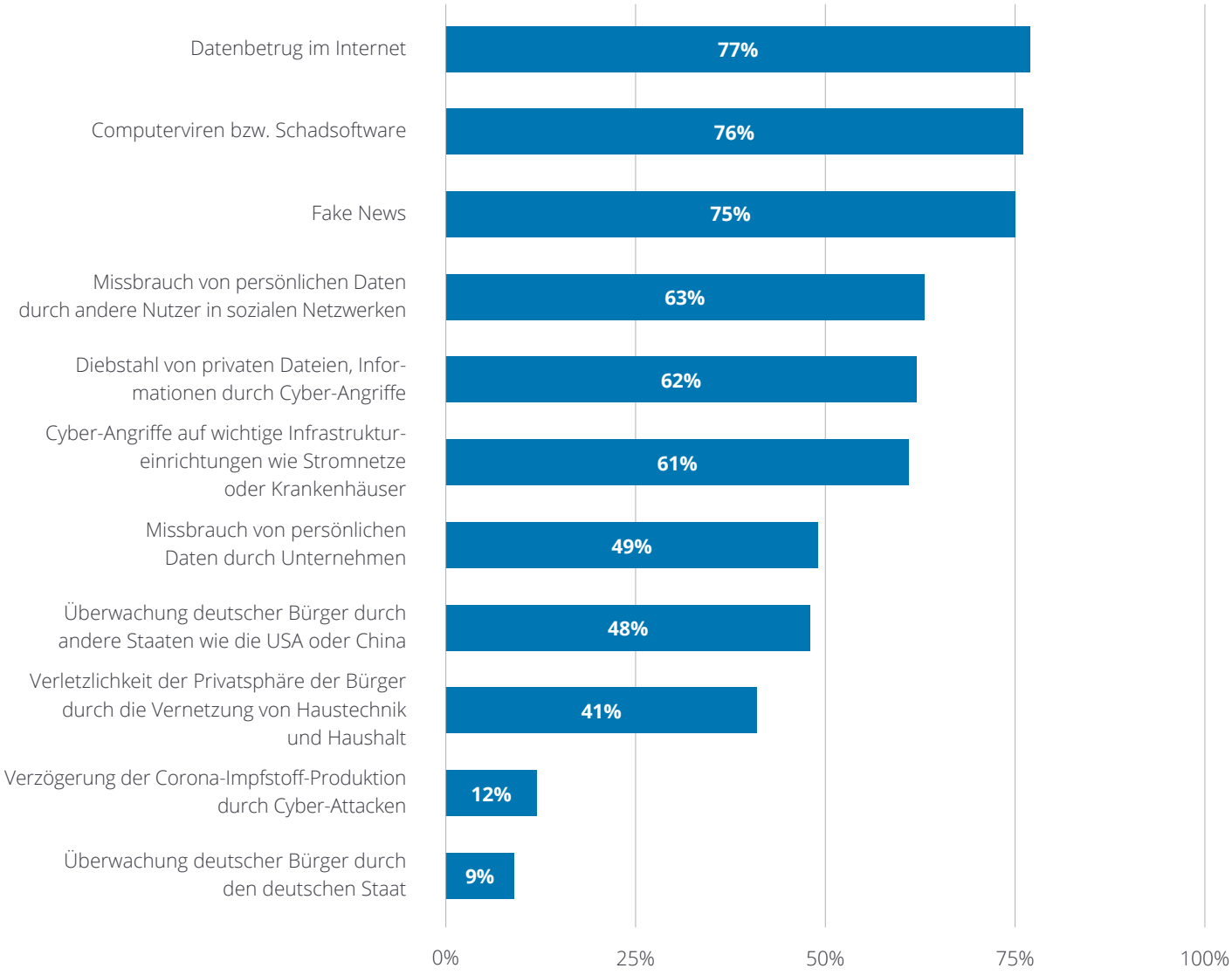
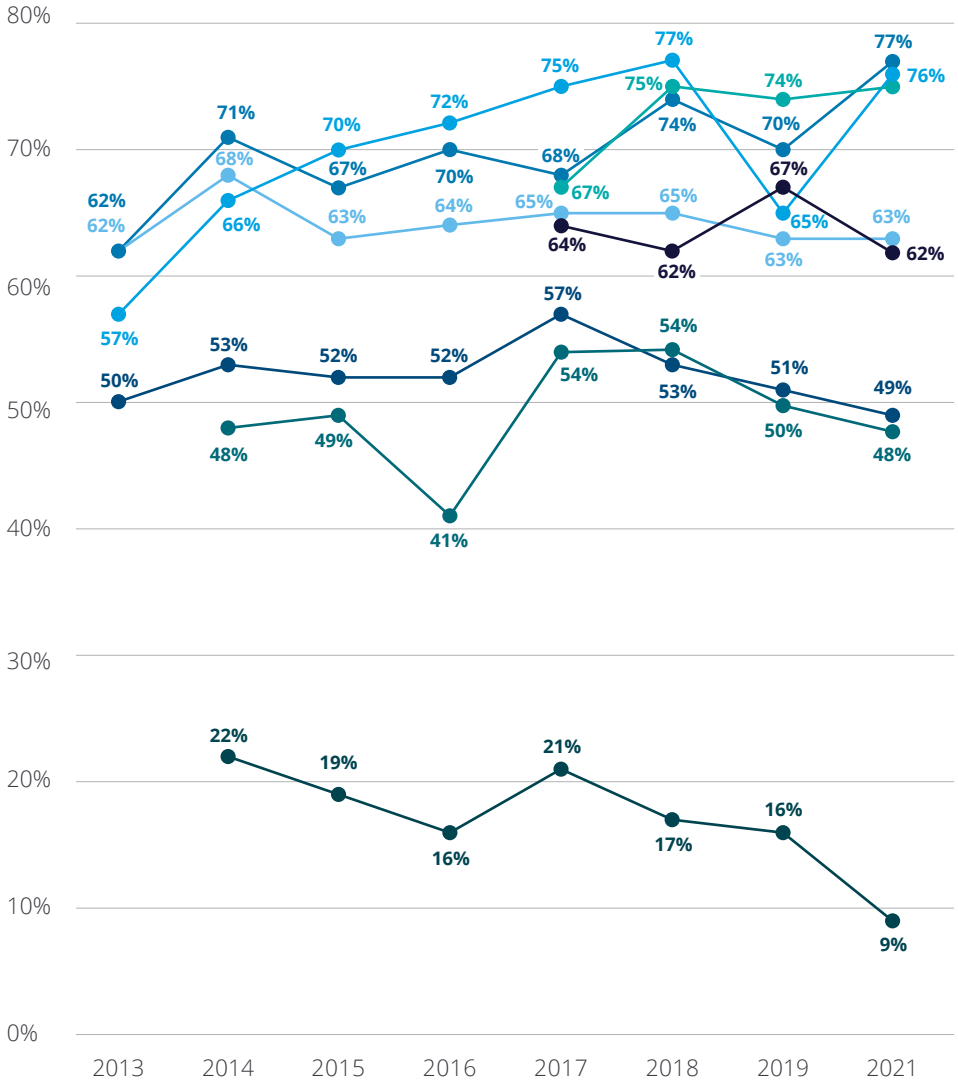


Abb. 2 – Entwicklungen der größten Cyber-Risiken in Deutschland seit 2013



- Datenbetrug im Internet
- Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken
- Computerviren bzw. Schadsoftware
- Missbrauch von persönlichen Daten durch Unternehmen
- Diebstahl von privaten Dateien, Informationen durch Cyber-Angriffe
- Fake News
- Überwachung deutscher Bürger durch andere Staaten wie die USA oder China
- Überwachung deutscher Bürger durch den deutschen Staat

Liegen die Top-3-Risiken dieses Jahr sehr eng beieinander, folgen mit etwas Abstand dahinter der Missbrauch persönlicher Daten durch andere Nutzer in sozialen Netzwerken (63 Prozent), der Diebstahl von privaten Dateien und Informationen durch Cyber-Angriffe (62 Prozent) sowie die Lahmlegung wichtiger Infrastruktureinrichtungen wie Stromnetze oder Krankenhäuser durch einen Cyber-Angriff (61 Prozent). Damit bewegt sich die Einschätzung dieser Risiken durch die Entscheidungsträger auf dem ungefähren Niveau von 2019.

Ähnlich wie 2019 sieht auch dieses Jahr rund die Hälfte der Befragten den Missbrauch von Daten durch Unternehmen als hohes Risiko, was Platz sieben in der Gefahrenrangliste bedeutet.

48 Prozent der Entscheidungsträger geben an, dass die Überwachung deutscher Bürger durch andere Staaten wie die USA oder China unverändert wie in den letzten Jahren ein hohes Risiko darstellt. Im Gegensatz dazu sehen lediglich neun Prozent der Entscheidungsträger eine Überwachung durch den eigenen Staat als hohes Risiko an, was den niedrigsten Wert seit Beginn der Umfrage im Jahre 2013 darstellt und gleichzeitig das Schlusslicht der abgefragten Risiken bildet.

Ein großes Risiko für die Privatsphäre der Bürgerinnen und Bürger sehen Entscheidungsträger dagegen in der zunehmenden Vernetzung der Haustechnik und von Haushaltsgeräten (41 Prozent). In der Verzögerung der Corona-Impfstoff-Produktion und -Auslieferung durch Cyber-Attacken sehen dagegen nur zwölf Prozent der Entscheidungsträger ein Risiko.

Betrachtet man die Top-5-Risiken seit Beginn der Befragung im Jahre 2013, lässt sich feststellen, dass die generelle Einschätzung der Cyber-Risiken allgemein auf einem konstant hohen Niveau bleibt – mit einer weiter steigenden Tendenz. Während 2013 keines der Top-Risiken über 62 Prozent kam, liegen 2021 die Top-3-Risiken jeweils bei 75 Prozent oder mehr. Insbesondere Datenbetrug im Internet stieg seit 2013 um 15 Prozentpunkte an. Während das Risiko Computerviren beziehungsweise Schadsoftware 2013 noch von 57 Prozent der Entscheidungsträger als hohes Risiko eingestuft wurde, stieg die Einschätzung 2021 um 19 Prozentpunkte auf 76 Prozent an. Interessanterweise liegt die diesjährige Einschätzung elf Prozentpunkte über dem Wert von 2019. Fake News liegen als Risikofaktor mit 75 Prozent einen Prozentpunkt über dem Wert von 2019 und sind seit Aufnahme in die Umfrage im Jahre 2017 um acht Prozentpunkte gestiegen. Der Diebstahl von privaten Dateien und Informationen durch Cyber-Angriffe verliert im Vergleich zu 2013 zwei Prozent und liegt sogar fünf Prozentpunkte unter dem Wert von 2019.

Die Entscheidungsträger aus Wirtschaft und Politik liegen bei der Bewertung der Risiken häufig sehr nah beieinander. Die größten Unterschiede lassen sich bei der Einschätzung des Risikos durch Computerviren beziehungsweise Schadsoftware erkennen. 79 Prozent der Wirtschaftsvertreter sehen hierbei ein großes Risiko, während 65 Prozent der Entscheidungsträger aus der Politik das so sehen.

Insbesondere in Hinsicht auf Einflussnahme, Beeinträchtigung und Vertrauen im Digitalen spielen die Top-Risiken im Wahljahr 2021 im gesamtgesellschaftlichen Kontext eine besondere Rolle. Datenbetrug im Internet, Computerviren und Fake News betreffen neben Unternehmen auch die einzelnen Bürger sowie die Gesellschaft als Ganzes. Das hohe Umfrageniveau dieser Risiken bei Entscheidungsträgern aus der Wirtschaft als auch aus der Politik verdeutlicht die Notwendigkeit, Cyber-Risiken als gesamtgesellschaftliche Herausforderung zu verstehen und gemeinsam anzugehen.

Risiken durch soziale Medien

Soziale Medien sind aus dem Alltag vieler Menschen nicht mehr wegzudenken. Netzwerke wie Facebook, LinkedIn und diverse andere verbinden Menschen weltweit miteinander. Die meisten Führungskräfte aus mittleren und großen Unternehmen haben eine positive Grundhaltung gegenüber sozialen Medien. So sehen 58 Prozent in ihnen eher Chancen als Risiken für ihre Unternehmen und Produkte. Diese Wahrnehmung hat seit 2019 leicht zugenommen.

Auch unter den befragten Abgeordneten sind 60 Prozent der Meinung, dass soziale Netzwerke den Politikern selbst mehr Chancen als Risiken bieten. Zeitgleich werden die Risiken, die von sozialen Medien ausgehen, zunehmend als Gefahr für die Demokratie wahrgenommen. Problematisch sehen Abgeordnete in dieser Hinsicht den zunehmenden Einfluss sozialer Medien auf die politische Meinungsbildung. Während noch im Jahr 2019 genau die Hälfte der Abgeordneten in sozialen Medien eher Risiken als Chancen für die Demokratie gesehen haben, sind es 2021 bereits 55 Prozent der Abgeordneten, die diese Ansicht teilen.

Als Risikofaktoren für die Demokratie und damit für die gesamte Gesellschaft werden unter anderem Fake News, Filterblasen, Shitstorms und Datenmissbrauchsfälle gesehen – Risiken, die im Zuge der Corona-Pandemie an Bedeutung gewonnen haben.

Abb. 3 – Chancen von sozialen Netzwerken

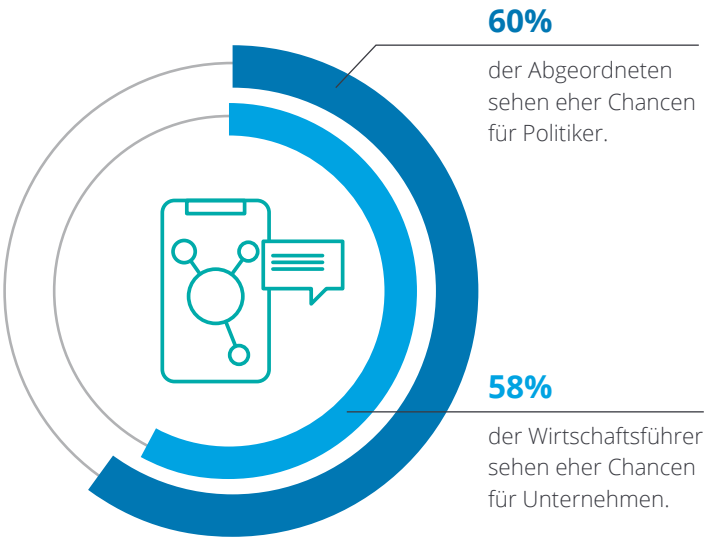
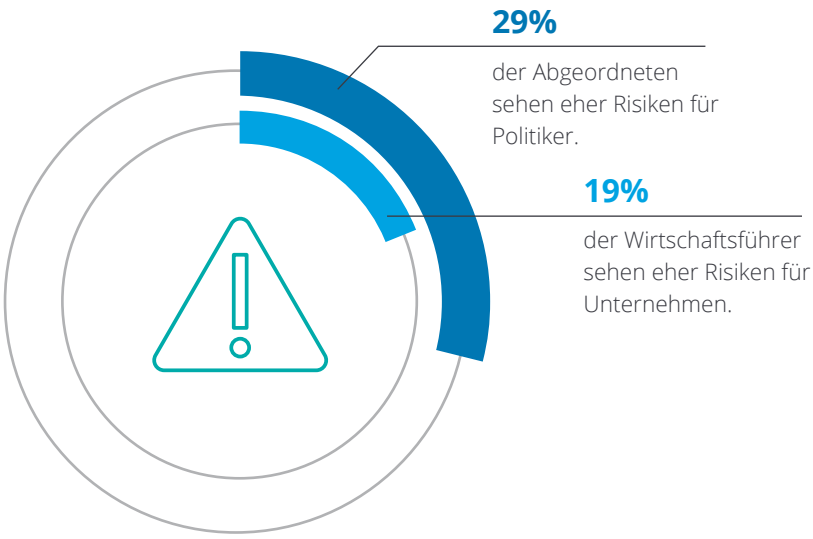


Abb. 4 – Risiken von sozialen Netzwerken

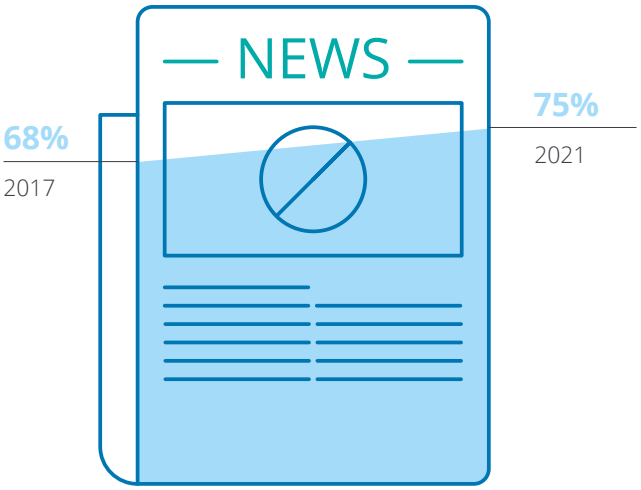


55%
der Abgeordneten sehen Risiko für Demokratie

Fake News
Als besonders große Gefahr wird die Manipulation der öffentlichen Meinung durch Fake News gesehen. 75 Prozent der Entscheidungsträger teilen diese Auffassung. Damit ist die Einschätzung der Gefährdungslage seit 2018 wieder auf einem Rekordhoch. Gegenüber 2017 bedeutet dies einen Zuwachs von sieben Prozentpunkten.

Im Wahljahr 2021, in dem eine durch die Corona-Pandemie beschleunigte Verlagerung des Wahlkampfes in das Internet stattfindet, spielt das Risiko digitaler Wahlmanipulation eine besonders wichtige Rolle. In diesem Zusammenhang hält auch Bundeswahlleiter Georg Thiel die Gefahr von Cyber-Angriffen zur Bundestagswahl für hoch.[1] Hier gebe es im Bereich IT eine Vielzahl an möglichen Risiken. Gemeinsam mit öffentlichen Rundfunkanstalten und den sozialen Medien wurden dafür entsprechende Vorkehrungen getroffen, um etwaige Falschmeldungen schnell richtigstellen zu können.

Abb. 5 – Fake News: ein großes Risiko in Deutschland seit 2017

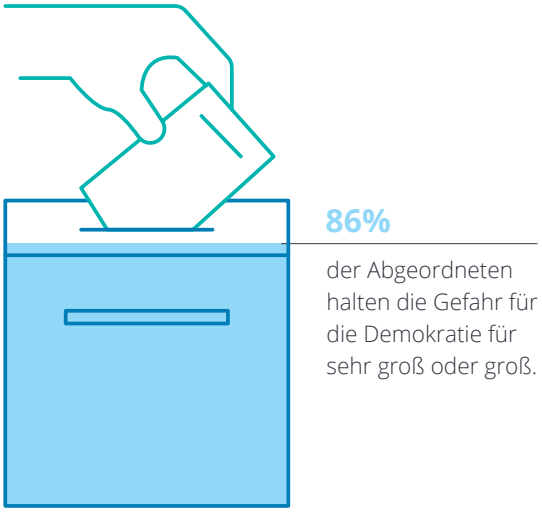


[1] Wahlleiter: Hohe Gefahr von Cyberangriffen zu Bundestagswahl, welt.de, 25.06.2021

Filterblasen

Ein weiteres Risiko, das durch die Nutzung sozialer Medien begünstigt wird, sind Filterblasen. Diese beschreiben das Phänomen, dass Teile der Bevölkerung zur Informationsgewinnung nur Medien- und vor allem Online-Angebote nutzen, die die eigene Meinung bestärken und daher nicht für andere Standpunkte erreichbar sind. Somit wird ein Hinterfragen der eigenen Position oder auch eine für die Demokratie erforderliche Auseinandersetzung mit anderen Standpunkten erheblich erschwert. 86 Prozent der Abgeordneten aus dem Deutschen Bundestag, den Landtagen und dem EU-Parlament sehen in Filterblasen eine sehr große oder große Gefahr für die Demokratie. Die Gefahr wird somit offenbar höher eingeschätzt als durch Fake News.

Abb. 6 – Filterblasen: eine große Gefahr für die Demokratie



„Soziale Netzwerke bieten eine nie zuvor dagewesene Fülle an Informationen und Meinungen verschiedenster Bevölkerungsgruppen. Ohne ein schärferes Bewusstsein der Nutzer bleibt diese Chance jedoch weitgehend ungenutzt, da sie innerhalb der Filterblasen häufig nur ihre eigene Meinung bestätigt sehen."

Marius von Spreti | Cyber Risk Leader, Deloitte

Shitstorms

Ein weiteres Phänomen im Internet und insbesondere in sozialen Medien sind Shitstorms. Dabei handelt es sich um eine Fülle von negativen Kommentaren und Beschimpfungen im Internet, welche sich auf Personen oder Organisationen beziehen. Wesentliche Treiber sind eine häufig auftretende Enthemmung sowie der Deckmantel der Anonymität. Hinzu kommen häufig Trolle, die die Auseinandersetzungen in sozialen Medien weiter befeuern und zur verbalen Eskalation beitragen. Als Trolle werden Personen bezeichnet, die vorsätzlich mit provokanten Kommentaren verbalen Streit entfachen und andere Nutzer verägern wollen. 15 Prozent der Wirtschaftsführer berichten davon, dass ihre Unternehmen schon Opfer eines Shitstorms im Internet geworden sind. Überdurchschnittlich häufig betroffen sind große Unternehmen mit 1.000 und mehr Mitarbeitenden, von denen 22 Prozent von mindestens einem solchen Vorfall in der Vergangenheit berichten. Kleine Unternehmen mit unter 100 Mitarbeitenden waren hingegen mit neun Prozent nicht einmal halb so häufig betroffen.

Im Vergleich zu Unternehmensvertretern sind Abgeordnete wesentlich häufiger von Shitstorms betroffen. Knapp jeder zweite Abgeordnete (49 Prozent) ist einem Shitstorm bereits mindestens einmal zum Opfer gefallen. Insgesamt 32 Prozent der Abgeordneten haben einen Shitstorm gegenüber ihrer eigenen Person bereits mehrfach erlebt.

So wie Abgeordnete öfter von Shitstorms betroffen sind als Unternehmen, verfolgen Abgeordnete sowie Parteien auch öfter, was in sozialen Medien über deren Partei geäußert wird. Während sich 68 Prozent der Abgeordneten darüber auf dem Laufenden halten, was in den sozialen Medien im Zusammenhang mit ihrer Partei geäußert wird, verfolgen nur 55 Prozent der Unternehmen systematisch, was in entsprechenden Medien im Zusammenhang mit ihrem Unternehmen berichtet wird. Auffällig ist hierbei, dass Unternehmen, welche in sozialen Medien eher Risiken als Chancen sehen, unterdurchschnittlich häufig (40 Prozent) systematisch verfolgen, was in sozialen Netzwerken über das Unternehmen geäußert wird.

Abb. 7 – Opfer von Shitstorms

Bereits mindestens einmal Opfer eines Shitstorms geworden sind:

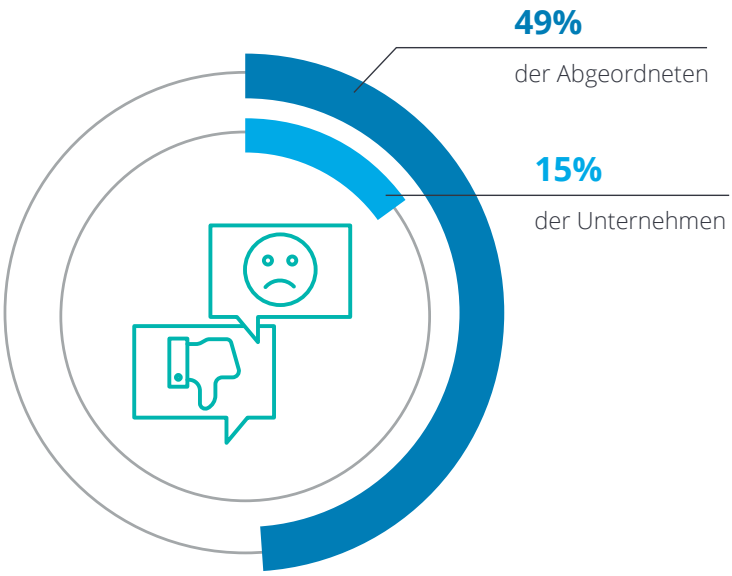
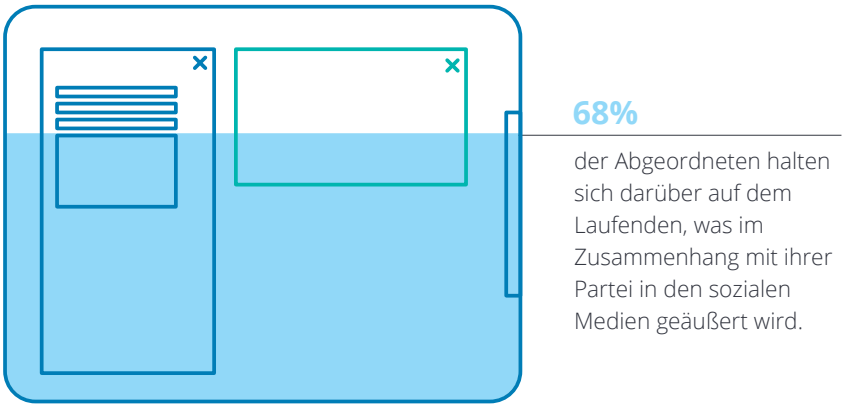


Abb. 8 – Politiker verfolgen mehrheitlich das Echo in sozialen Medien



Um die Gefahr durch Shitstorms zu minimieren, sind die Überwachung von Aktivitäten in Social-Media-Plattformen sowie die Sensibilisierung von Teammitgliedern sowohl für Wirtschaftsführer als auch Politiker unumgänglich. In diesem Zusammenhang empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Leitfaden für soziale Netzwerke[2] den Unternehmen, die Aktivitäten Dritter zu beobachten. In dem Leitfaden für Kandidierende für Bundes- und Landeswahlen empfiehlt das BSI zudem, Wahlkampfteams hinsichtlich potenzieller Gefährdungen zu sensibilisieren.[3]

Shitstorms können durch ihre destruktive Wirkung in Form von Fehl- oder Desinformation massive Auswirkungen für die Gesellschaft und Demokratie, aber auch das Individuum und den Markt haben. Aus Furcht vor potenziellen Shitstorms werden zum einen politische Debatten gelähmt und zum anderen Minderheitsmeinungen zunehmend zurückhaltend öffentlich kommuniziert.

Zusätzlich bieten Shitstorms das Potenzial für Imageschäden und Lynchjustiz-Fälle, in denen Individuen oder Organisationen voreilig und oftmals unberechtigterweise von einer aufgebrachten Masse verurteilt oder boykottiert werden. Nicht zuletzt kann dies für Unternehmen neben Reputationsverlusten auch zu erheblichen finanziellen Folgen führen.

Abb. 9 – Politiker verfolgen mehrheitlich das Echo in sozialen Medien

Es wird systematisch nachverfolgt, was in sozialen Netzwerken über das Unternehmen geäußert wird.

55%

der Wirtschaftsführer insgesamt geben das an.

40%

der Wirtschaftsführer, die eher Risiken in sozialen Medien für ihr Unternehmen sehen, geben das an.

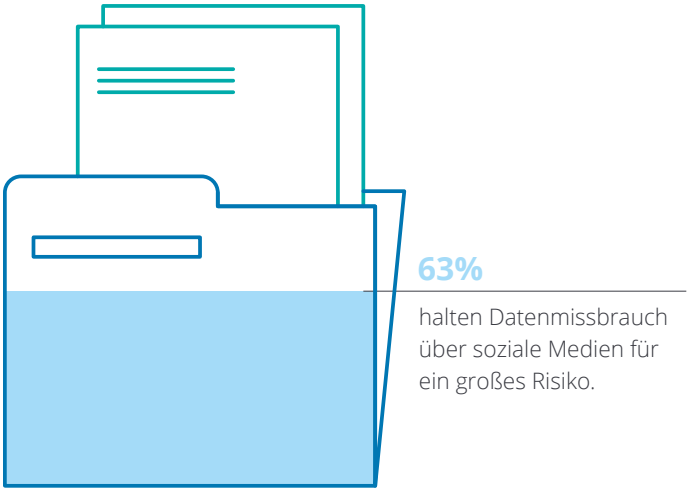
[2] Empfehlung: IT im Unternehmen – Soziale Medien & Soziale Netzwerke, BSI, Juni 2021
[3] IT-Sicherheitsleitfaden für Kandidierende bei Bundes- und Landeswahlen, BSI, Juni 2021

Als ebenfalls große Gefahr wird der Datenmissbrauch im Zusammenhang mit sozialen Netzwerken gesehen. 63 Prozent der Entscheidungsträger geben an, dass der Missbrauch von persönlichen Daten durch andere Nutzer ein großes Risiko für die Menschen in Deutschland darstellt.

Auch Phänomene wie Fake News, Filterblasen und Shitstorms stellen für die Befragten ein Risiko für die gesamte Gesellschaft dar.

Um diesen Risiken entgegenzuwirken, bedarf es nicht nur entsprechender rechtlicher und politischer Rahmenbedingungen. Genauso wichtig ist das verantwortungsvolle Handeln jedes Einzelnen als Teil der Gesellschaft. Die Verantwortung begrenzt sich dabei nicht nur auf die Nutzung sozialer Medien im privaten Umfeld. Auch am Arbeitsplatz stehen Menschen im Visier von Angreifern. Bedachtes Handeln gewann auch durch die Verlagerung des Arbeitsplatzes in das Homeoffice während der Corona-Pandemie an Bedeutung.

Abb. 10 – Datenmissbrauch: ein großes Risiko in Deutschland



„Auch wenn eine umfassende Risikoeliminierung nie möglich ist, beginnt der Schutz vor zunehmendem Datenmissbrauch in den Köpfen und an den Endgeräten der Anwender."

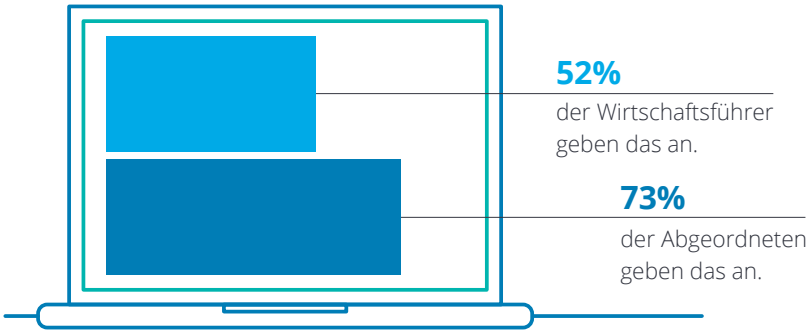
Marius von Spreti | Cyber Risk Leader, Deloitte

Herausforderungen durch die Corona-Pandemie

Seit Beginn der Corona-Pandemie hat sich das Arbeiten im Homeoffice in mittleren und großen Unternehmen und noch ausgeprägter in der Politik etabliert. 52 Prozent der Wirtschaftsführer und 73 Prozent der Abgeordneten geben an, dass in dieser Zeit viele ihrer Mitarbeiter von zu Hause aus gearbeitet haben. Das verbreitete Arbeiten im Homeoffice stellt auch neue Anforderungen an die Cyber-Sicherheit. Die hohe Anzahl der IT-Systeme im Homeoffice, ihre Verbindung miteinander und mit dem Unternehmensnetz sowie die verstärkte Nutzung von Kollaborationstools bieten eine vergrößerte Angriffsfläche gegenüber Cyber-Angriffen und müssen geschützt werden. Zudem nutzen Angreifer die Unsicherheit und das Informationsbedürfnis von Menschen während dieser Zeit gezielt für kriminelle Handlungen aus. Verantwortungsbewusstes Handeln eines jeden Einzelnen wird damit noch wichtiger.

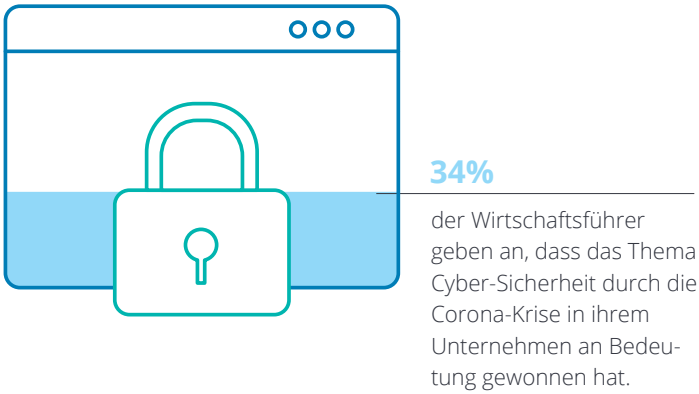
Abb. 11 – Verbreitung von Homeoffice seit Beginn der Corona-Pandemie

Seit Beginn der Corona-Krise haben viele Mitarbeiter von zu Hause aus gearbeitet.



34 Prozent der befragten Wirtschaftsführer geben an, dass Cyber-Sicherheit durch die Corona-Krise in ihrem Unternehmen an Bedeutung gewonnen hat.

Abb. 12 – Bedeutung der Cyber-Sicherheit in der Corona-Krise



In diesem Zusammenhang geben außerdem 82 Prozent der Wirtschaftsführer und 52 Prozent der Abgeordneten an, dass spezielle IT-Sicherheitsmaßnahmen wie die Durchführung von Schulungen, die Installation spezieller Sicherheitssoftware oder die Sperrung bestimmter Anwendungen für die Mitarbeiter im Homeoffice getroffen wurden.

Das Risiko, das von Mitarbeitenden im Homeoffice ausgeht, wird insgesamt als eher gering eingeschätzt. 71 Prozent der Führungskräfte aus der Wirtschaft und 84 Prozent der Abgeordneten halten die Risiken für weniger groß oder sehen kein zusätzliches Risiko.

Abb. 13 – Spezielle IT-Sicherheitsmaßnahmen für Mitarbeiter im Homeoffice

Es wurden spezielle IT-Sicherheitsmaßnahmen für Mitarbeitende im Homeoffice getroffen.

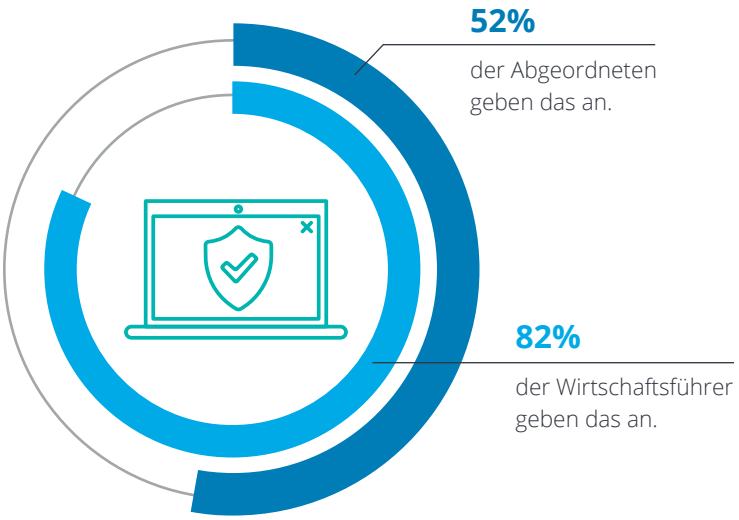
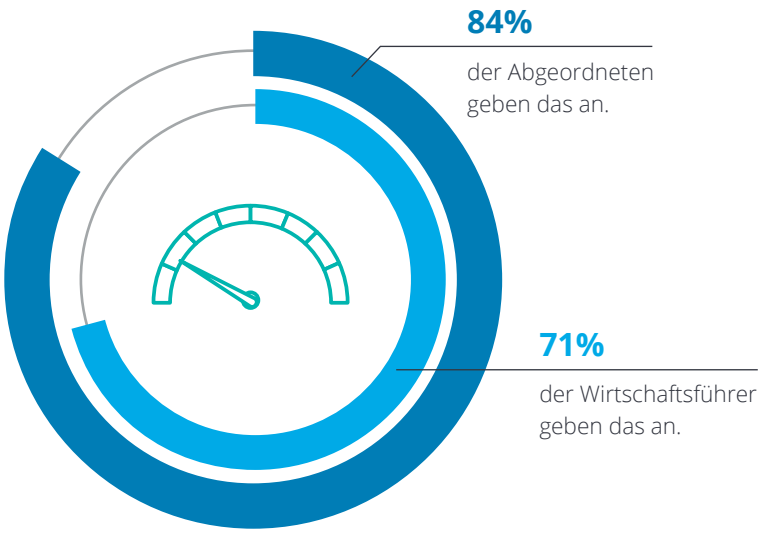


Abb. 14 – Geringes zusätzliches Risiko durch Mitarbeiter im Homeoffice

Das zusätzliche Risiko, welches von Mitarbeitern im Homeoffice ausgeht, ist weniger groß oder nicht existent.



Gleichzeitig haben jedoch 34 Prozent der Wirtschaftsführer und 22 Prozent der Abgeordneten Zweifel am Risikobewusstsein ihrer Mitarbeiter.

Die starke Verbreitung der Arbeit im Homeoffice führte auch zu einer verstärkten Nutzung von digitalen Kollaborations- und Kommunikationstools. 83 Prozent der Wirtschaftsführer und 97 Prozent der Abgeordneten geben beispielsweise eine (sehr) intensive Nutzung von Videokonferenzen an.

Das Risiko, das von Videokonferenztools für die IT-Sicherheit ausgeht, wird als eher gering eingeschätzt. 67 Prozent der Wirtschaftsführer und 59 Prozent der Abgeordneten beurteilen das Risiko als weniger groß oder gar nicht groß. Allerdings bestehen bei 56 Prozent der Abgeordneten und bei 48 Prozent der Wirtschaftsführer Vorbehalte gegenüber Videokonferenztools aus den USA hinsichtlich des Datenschutzes und der Datensicherheit. Diese Skepsis lässt darauf schließen, dass das Niveau der Datenschutzstandards in den USA als geringer eingeschätzt wird als in Deutschland oder in der Europäischen Union. Im Kontext der Datensicherheit könnte dies als Hinweis auf die Angst vor Spionage durch US-Dienste gedeutet werden. Trotz einer ausreichenden Anzahl an Videokonferenztools konnte sich bisher keine deutsche oder europäische Alternative zu Zoom, Microsoft Teams, Skype oder Cisco WebEx flächendeckend durchsetzen. Dies könnte unter anderem auf die fehlende Bekanntheit zurückzuführen sein, die einen wesentlichen Erfolgsfaktor darstellt.

Nicht nur im Bereich der Videokonferenztools kommen die marktführenden Anbieter aus anderen Staaten als Deutschland oder der Europäischen Union. Auch im Bereich absoluter Schlüsseltechnologien wie beispielsweise 5G kommen viele Lösungen aus den USA oder China. In diesem Zusammenhang stellt sich die Frage nach der Wettbewerbsfähigkeit Deutschlands und der EU.

Abb. 15 – Zweifel am Risikobewusstsein der Mitarbeiter im Homeoffice

Es bestehen Zweifel am Risikobewusstsein von Mitarbeitern im Homeoffice.

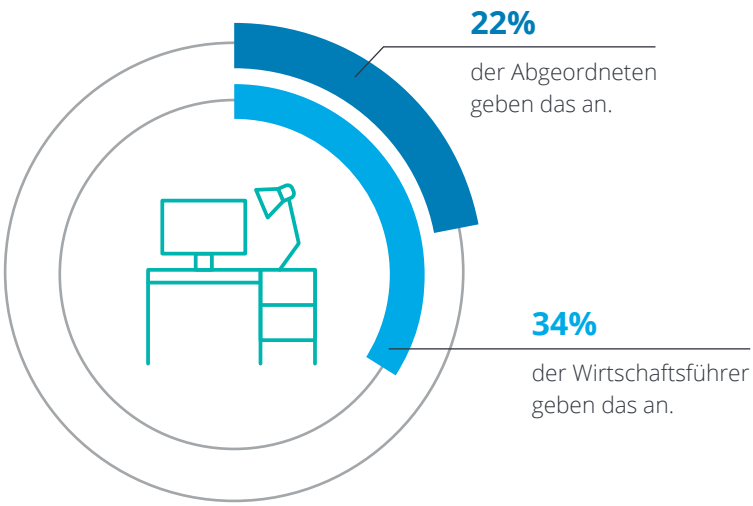


Abb. 16 – Nutzung von Videokonferenzen

Videokonferenzen werden während der Corona-Pandemie sehr intensiv oder intensiv genutzt.

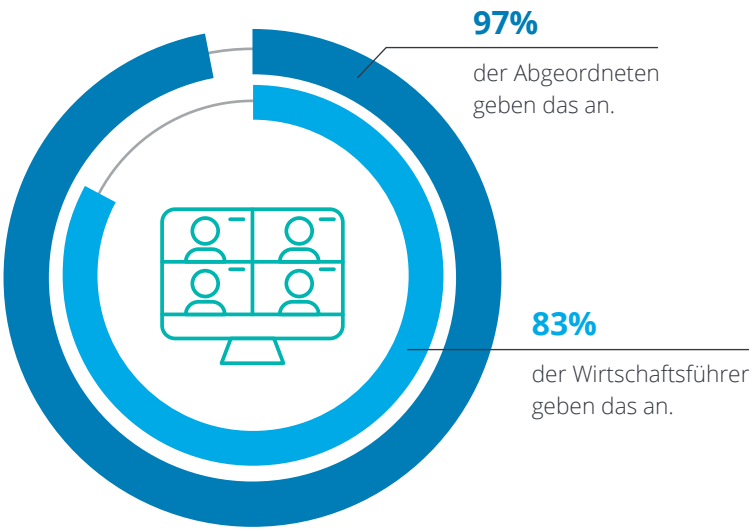


Abb. 17 – IT-Risiken durch die Nutzung von Videokonferenztools

Es bestehen große oder sehr große Risiken durch die Nutzung von Videokonferenztools.

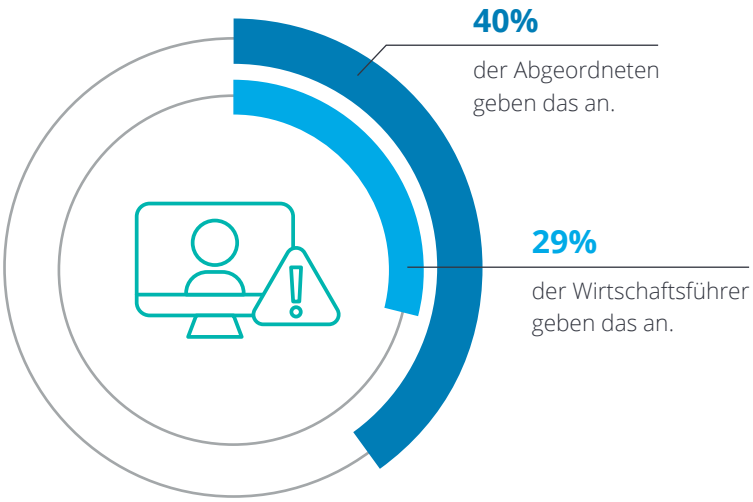
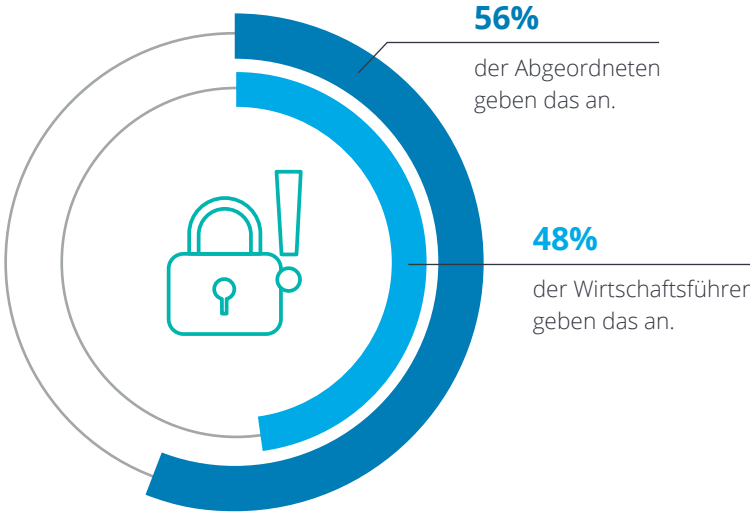


Abb. 18 – Vorbehalte gegenüber Videokonferenztools aus den USA

Es bestehen Bedenken hinsichtlich des Datenschutzes und der Datensicherheit gegenüber Videokonferenztools aus den USA.



Schlüsseltechnologien für Cyber-Sicherheit

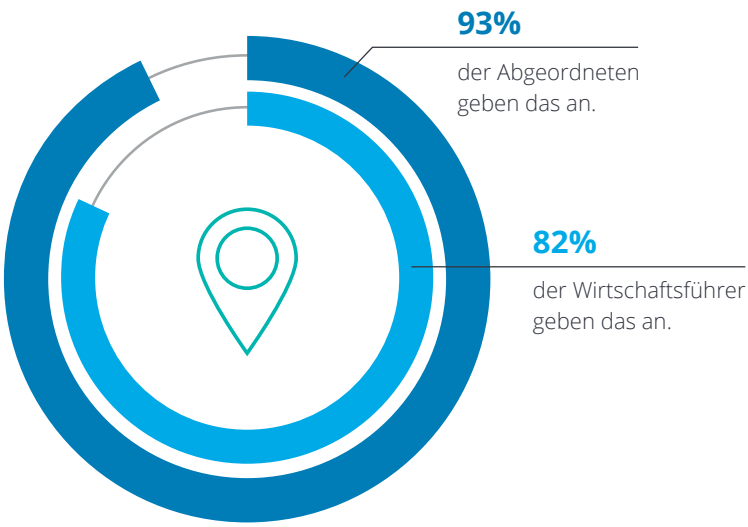
Schlüsseltechnologien sind der Treiber der Zukunft. Aufgrund ihrer volkswirtschaftlichen Hebelwirkung sind sie von besonderer Bedeutung für die Zukunftsfähigkeit einer Gesellschaft. Die Förderung von Schlüsseltechnologien trägt dazu bei, die Wettbewerbsfähigkeit der deutschen Industrie auf dem internationalen Parkett zu stärken. Hierzu fördert die Bundesregierung Kompetenzen in Schlüsseltechnologien wie IT-Sicherheit, KI, Mikroelektronik oder Quantentechnologien.[4]

Damit einhergehend erachtet es die große Mehrheit der Befragten für die Cyber-Sicherheit in Deutschland als notwendig, dass wichtige Schlüsseltechnologien für die Digitalisierung und Vernetzung von deutschen oder europäischen Unternehmen hergestellt werden. Damit soll eine größere Unabhängigkeit von anderen Ländern sichergestellt werden. Dies gaben 82 Prozent der Führungskräfte aus der Wirtschaft und 93 Prozent der Abgeordneten an. Dies bedeutet eine Steigerung um elf Prozentpunkte unter den Wirtschaftsführern und um vier Prozent unter den Abgeordneten gegenüber 2019.

Dieser breite Konsens sollte die Grundlage für eine enge Zusammenarbeit zwischen der Wirtschaft und der Politik bei der Förderung von Forschungs- und Entwicklungsaktivitäten zur Entwicklung von Schlüsseltechnologien in Deutschland und Europa bilden.

Abb. 19 – Bedarf an in der EU produzierten Schlüsseltechnologien

Schlüsseltechnologien sollten in der EU produziert werden.



„Cyber-Sicherheit ist das Fundament für digitale Souveränität. Die Entwicklung von Schlüsseltechnologien für die Cyber-Sicherheit durch deutsche beziehungsweise europäische Unternehmen ist damit eine Grundvoraussetzung, wenn wir in Zukunft selbstbestimmt werden wollen."

Peter Wirnsperger | Lead Civil Government, Deloitte

[4] Bundesbericht Forschung und Innovation 2020.

Zusammenarbeit von Politik und Wirtschaft

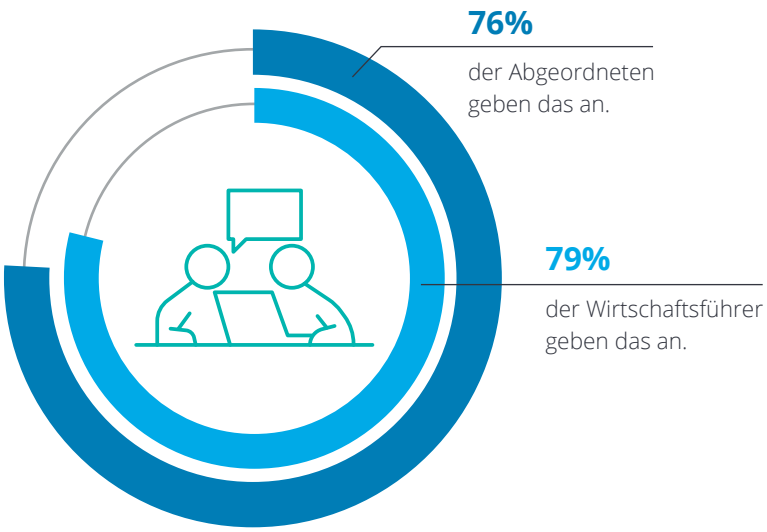
Um ein stabiles Fundament für die deutsche und europäische IT-Wirtschaft zu schaffen, ist eine zielgerichtete und nachhaltige Zusammenarbeit von Wirtschaft und Politik unabdingbar. Gegenüber den Umfrageergebnissen aus dem Cyber Security Report 2019 hat sich das Meinungsbild diesbezüglich nicht verändert. Nach wie vor wird der Austausch zwischen staatlichen Stellen und Wirtschaft als nicht ausreichend empfunden. Knapp 80 Prozent der Abgeordneten und Wirtschaftsführer geben das in diesem Jahr an. Dabei stellt sich die Frage, ob seitdem keine ausreichenden Maßnahmen zur Intensivierung der Zusammenarbeit getroffen wurden oder ob die getroffenen Maßnahmen nicht die gewünschte Wirkung erzielen.

Mangelnder Informationsaustausch

Die Wirtschaft sieht ihre Bedürfnisse durch die Politik im Bereich der Cyber-Sicherheit nur ungenügend befriedigt, was gut zwei Drittel der Befragten angaben. Diese Einschätzung bestätigen auch die Antworten der Abgeordneten mehrheitlich. Es mangelt an klaren Hilfestellungen und Anweisungen auf der Basis der aktuellen technologischen Entwicklungen.

Abb. 20 – Mangelnder Austausch zum Thema IT-Sicherheit zwischen Wirtschaft und Politik

Es müsste einen stärkeren Austausch zwischen staatlichen Stellen und Privatwirtschaft zum Thema Cyber-Sicherheit geben.



Ein Großteil der befragten Abgeordneten von 58 Prozent gibt an, sich nur weniger gut oder gar nicht gut über die Bedürfnisse der Wirtschaft informiert zu fühlen. Im Vergleich zu den Antworten aus dem Jahr 2019 ist das ein Anstieg von acht Prozentpunkten. Vor zwei Jahren fühlten sich demnach 49 Prozent der Abgeordneten weniger gut oder gar nicht gut über die Probleme und Bedürfnisse der Wirtschaft informiert.

Etwaige Auskünfte zu Fragen der Cyber-Sicherheit erhalten die befragten Abgeordneten aus ihrem eigenen Umfeld und halten daher insbesondere Informationen von Behörden, vom wissenschaftlichen Dienst des Bundestages oder aus den Fraktionen für besonders zuverlässig. Nur zwei Prozent verlassen sich hier auf die Zuverlässigkeit der Unternehmen. Daraus kann der Eindruck entstehen, dass keine der beiden Seiten sich aktiv bemüht, einen nachhaltigen Austausch zu initiieren.

Abb. 21 – Politischer Umgang mit Bedürfnissen aus der Wirtschaft

Zusammenspiel zwischen Politik und Wirtschaft

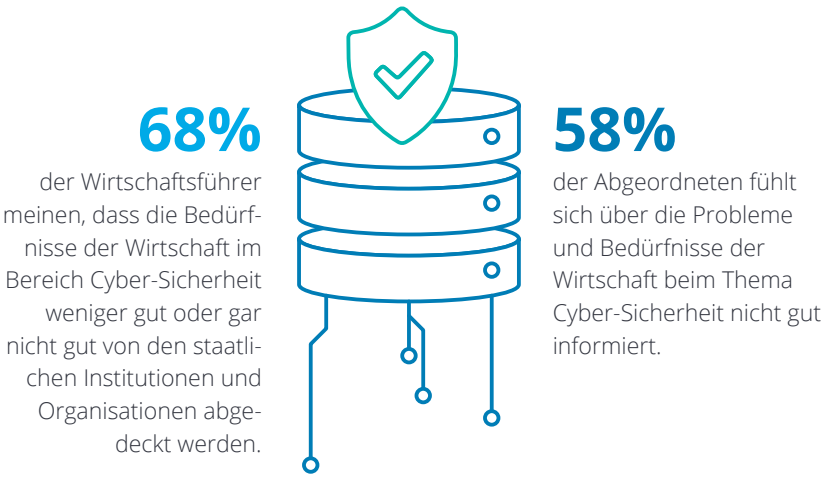
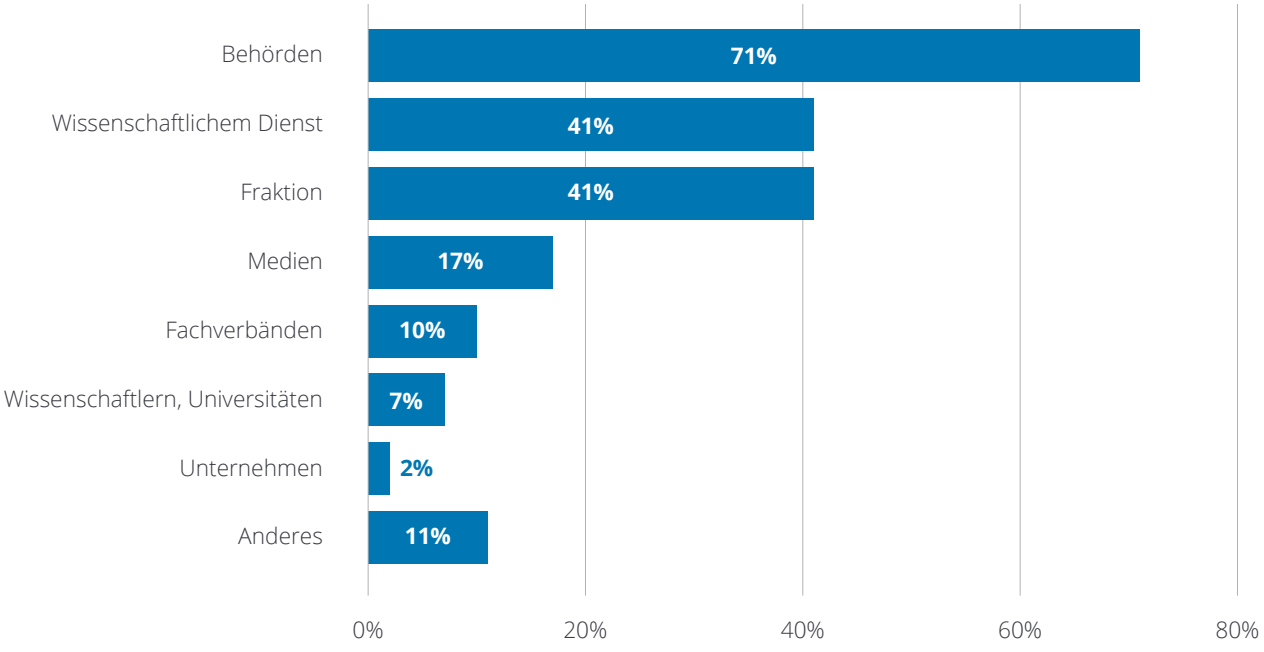


Abb. 22 – Zuverlässige Informationen zum Thema Cyber-Sicherheit

Abgeordnete setzten beim Thema Cyber-Sicherheit vor allem auf Informationen von:



„Es ist alarmierend, dass sowohl Politiker als auch Wirtschaftsvertreter den gemeinsamen Austausch zur Erhöhung der Cyber-Sicherheit als nicht ausreichend wahrnehmen.“

Peter Wirnsperger | Lead Civil Government, Deloitte

Staatliche Maßnahmen

Darüber hinaus ist die Qualität der Umsetzung von Maßnahmen zur Verbesserung der Rahmenbedingungen für Cyber-Sicherheit zu nennen. Fast drei Viertel der Wirtschaftsführer wünschen sich beispielsweise eine stärkere Zentralisierung staatlicher Stellen beim Thema Cyber-Sicherheit, um einen einheitlichen Ansprechpartner für ihre Belange zu haben. Insbesondere große Unternehmen mit 1.000 und mehr Mitarbeitenden sehen hier Nachbesserungsbedarf und geben an, dass eine zentrale Anlaufstelle wichtig oder sehr wichtig sei.

In diesem Zusammenhang sprachen sich 72 Prozent der Wirtschaftsführer dafür aus, die Zuständigkeiten beim Thema Cyber-Sicherheit stärker zu zentralisieren und die aktuelle Aufteilung weniger föderal zu gestalten. Zum einen würde dadurch die Verteilung der Zuständigkeiten klarer strukturiert. Zum anderen würde es Vertrauen in die zuständigen Behörden schaffen und die Meldestruktur zur Anzeige von Sicherheitsvorfällen für die Wirtschaft vereinfachen.

Die befragten Abgeordneten sehen hier weniger Handlungsbedarf. 48 Prozent sind der Ansicht, dass die Zuständigkeiten gut zwischen Bundes- und Landesebene aufgeteilt sind.

Abb. 23 – Bedeutung einer zentralen staatlichen Anlaufstelle für Cyber-Sicherheit in der Wirtschaft

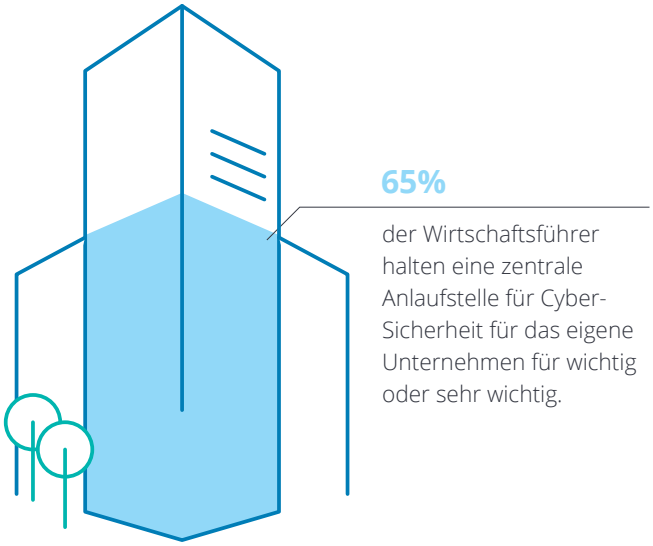
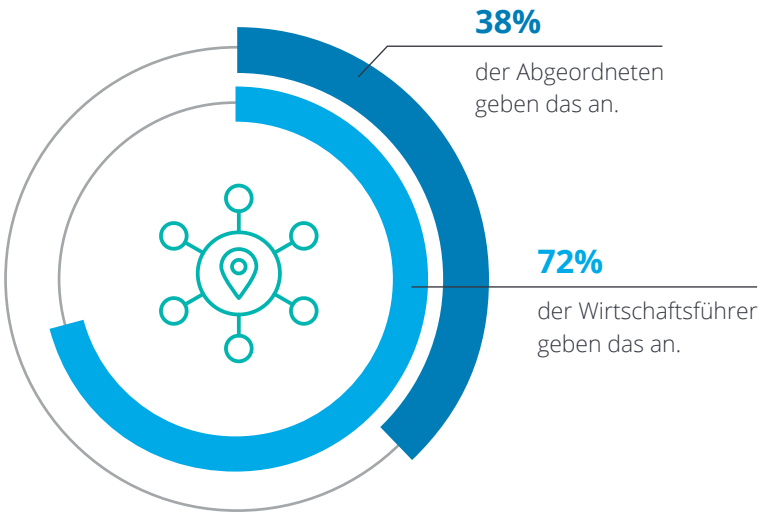


Abb. 24 – Föderale Arbeitsteilung vs. stärkere Zentralisierung

Die Zuständigkeit staatlicher Stellen beim Thema Cyber-Sicherheit sollte stärker zentralisiert werden.



Rund ein Drittel der großen und mittleren Unternehmen hatte bereits Kontakt zu staatlichen Stellen. Mehr als jedes dritte äußerte sich mit der erhaltenenBeratung oder Hilfe weniger oder gar nicht zufrieden.

Mehrheitlich als angemessen wahrgenommen wird die Regulierungsdichte sowohl im Bereich der Cyber-Sicherheit sowie auch im Bereich der Datensicherheit. Trotzdem hält jedoch rund ein Drittel der befragten Politiker und Wirtschaftsführer die Regulierung im Bereich der Cyber-Sicherheit für nicht ausreichend. Im Bereich der Datensicherheit unterscheidet sich die Meinung beider Gruppen. Während rund 30 Prozent der Wirtschaftsführer die Regulierungsdichte dort als zu hoch empfinden, sehen das nur rund 10 Prozent der befragten Politiker so. Knapp 30 Prozent nehmen zu wenig Regulierung in dem Bereich Datensicherheit wahr.

Abb. 25 – Unzufriedenheit mit staatlicher Beratung

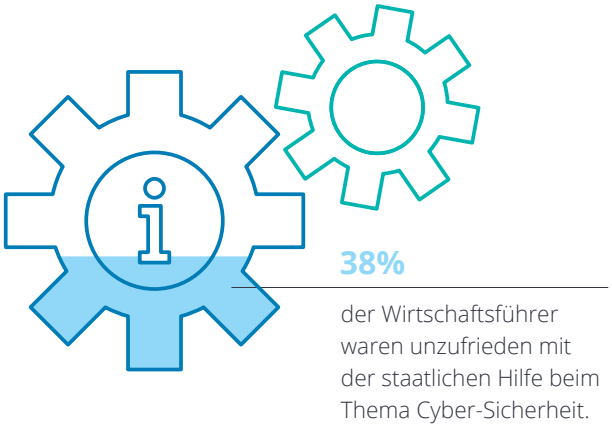
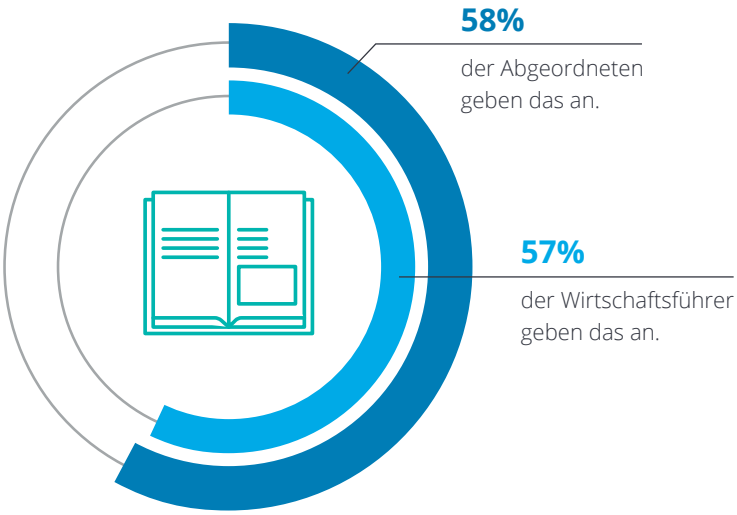


Abb. 26 – Angemessenheit der Regulierungsdichte im Bereich Cyber-Sicherheit

Im Bereich Cyber-Sicherheit ist die Regulierungsdichte angemessen.



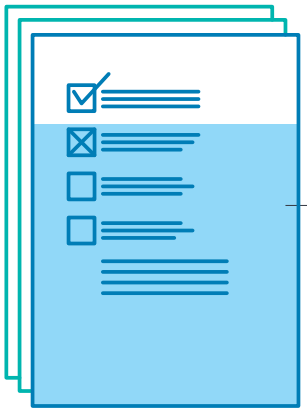
Der Beitrag der gesetzlichen Regelungen zur Cyber-Sicherheit für Unternehmen wird von beiden Seiten eher als gering veranschlagt. So gaben 76 Prozent der Entscheidungsträger an, dass die gesetzlichen Regelungen in Deutschland zur Cyber-Sicherheit gar nichts oder nur etwas beitragen.

Nicht DASS reguliert wird, sondern WO, ist demnach für die Befragten von entscheidender Bedeutung.

Hier ist abermals eine Diskrepanz in der Betrachtungsweise der beiden Teilnehmergruppen erkennbar. Diese ist nicht zuletzt auch auf einen mangelnden Austausch und Wissenstransfer zurückzuführen. Bisher scheint es kein ausreichendes Verständnis über die Ausgangslage des jeweils anderen zu geben, eine Grundvoraussetzung, um sich einander zu nähern.

Auf die Herausforderung einer zielführenden Zusammenarbeit zwischen Wirtschaft und Politik zahlt auch der aktuelle Entwurf der Fortführung der Cyber-Sicherheitsstrategie[5] der Bundesregierung ein, welcher von einem „Gemeinsamen Auftrag von Staat und Wirtschaft" spricht, „die Kooperation von Staat und Wirtschaft" stärken möchte und darüber hinaus auch darauf abzielt Maßnahmen zu erarbeiten, um die bereits bestehende Kooperation auszubauen.

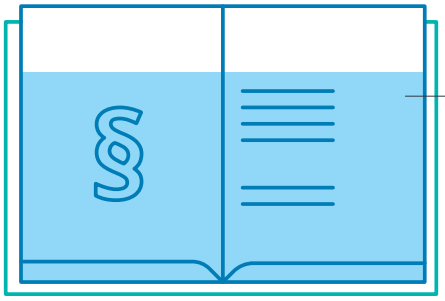
Abb. 27 – Angemessenheit der Regulierungsdichte im Bereich Datenschutz



76%

der Wirtschaftsführer geben an, dass der Staat im Bereich Datenschutz zu viele Vorschriften macht oder den falschen Bereich kontrolliert.

Abb. 28 – Wirkung der Regelungen im Bereich Cyber-Sicherheit



76%

der Entscheidungsträger geben an, dass gesetzliche Regelungen zur Erhöhung der Cyber-Sicherheit von Unternehmen gar nichts oder nur etwas beitragen.

„Die Befragung macht deutlich, dass es Nachholbedarf hinsichtlich des Austauschs zwischen Staat und Wirtschaft gibt. Nun ist es an der Zeit, die nötigen Maßnahmen umzusetzen und ein stabiles Fundament für die deutsche und europäische IT-Wirtschaft zu schaffen."

Peter Wirnsperger | Lead Civil Government, Deloitte

[5] Entwurf der Cybersicherheitsstrategie für Deutschland 2021, bmi.bund.de, 09.06.21

Mögliche Handlungsfelder

Der erfolgreiche Aufbau von Cyber-Sicherheit in Deutschland bedeutet, dass jede Gesellschaftsgruppe und jede/r Einzelne gefragt sind, ihren bzw. seinen Beitrag zu leisten. Die Befragung hat gezeigt, dass es nur im Zusammenspiel aller beteiligten Akteure gelingt, die zunehmend komplexer und dynamischer werdenden Anforderungen zu meistern. Die bevorstehende Bundestagswahl 2021 birgt einmal mehr die Chance, hier an den richtigen Stellschrauben zu drehen und gute Rahmenbedingungen für eine erfolgreiche deutsche Cyber-Sicherheit zu gestalten.

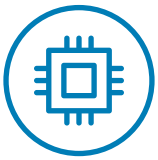
Aus der Befragung haben sich für Deloitte die folgenden möglichen Handlungsfelder ergeben.

Handlungsfeld 1
Internet- und Medienkompetenz stärken

Fake News und Meinungsmanipulationen aktiv entgegenwirken
Meinungsmanipulationen und Fake News stellen eine konstante Gefährdung des demokratischen Prozesses und für die Reputation von Unternehmen dar. Gerade in Krisen wie der aktuellen Corona-Pandemie verbreiten sich Fake News umso rasanter und erreichen immer mehr Menschen. Dies erfordert fortlaufende Sensibilisierung, Überwachung und proaktives Management der Kommunikationskanäle. Der erste Ansatzpunkt diesbezüglich sollte sein, aktiv zu verfolgen, was über das eigene Unternehmen oder die eigene Institution in den sozialen Medien berichtet wird. Dazu gehört auch das kritische Überprüfen von Informationsquellen; zur Verifikation können auch moderne Instrumente aus Data Analytics oder KI eingesetzt werden.

Sensibilisierung im Bereich Cyber-Sicherheit intensivieren
Cyber-Sicherheit betrifft jeden. Angesichts der Flut an Informationen, mit der jeder täglich konfrontiert wird, erscheinen Bürgerinnen und Bürger zunehmend überfordert. Nur wenige sind sich der Gefahren im Cyber-Raum bewusst und wissen sich effektiv gegen diese zu schützen. Aus diesem Grund spielt die Aufklärung in den Bereichen Cyber-Sicherheit und kritische Medienkompetenz eine essenzielle Rolle zur Bekämpfung von Cyber-Kriminalität und Beeinflussung der öffentlichen Meinung. So sollten diese Themen fester Bestandteil der Schulbildung und in Ausbildungsberufen werden. Darüber hinaus gilt es, zielgerichtete Schulungs- und Weiterbildungsmaßnahmen für Führungskräfte zu etablieren, damit diese informierte Entscheidungen treffen können. Da das Wissen im Bereich der Cyber-Sicherheit sehr schnell veraltet wird, müssen Sensibilisierungs- und Weiterbildungsmaßnahmen kontinuierlich aktuell gehalten werden.

Die Gefahren von Social Media gezielt adressieren
Shitstorms und Filterblasen, vor allem in sozialen Medien zu finden, bergen die Gefahr von Reputationsverlust, einem eingeschränkten Meinungsaustausch bis hin zu finanziellen Schäden. Für Unternehmen empfiehlt es sich, sowohl präventive als auch reaktive Vorbereitungsmaßnahmen für den Fall eines Shitstorms zu treffen. Das Zurechtlegen einer Kommunikationsstrategie verleiht zusätzlich Kontrolle über die Situation. Zur Vermeidung von Shitstorms und Filterblasen sollten auch die Betreiber sozialer Netzwerke in die Pflicht genommen werden, welche ebenfalls vorbeugende Maßnahmen entwickeln sollten. Politiker und Parteien sollten den sachlichen Meinungsaustausch in den Vordergrund stellen und starker Polarisierung entgegenwirken. Zudem sollte es mehr politische Aufklärung durch staatliche Institutionen, Verbände und Stiftungen geben, um ein größeres Bewusstsein für Phänomene wie Filterblasen zu schaffen.



Handlungsfeld 2
Technologische Unabhängigkeit fördern

Gezielte Förderung von Forschungs- und Entwicklungsaktivitäten
Forschungs- und Entwicklungsaktivitäten in strategisch relevanten Bereichen und zu Schlüsseltechnologien sollten gefördert werden. Im Sinne einer gesamtgesellschaftlichen Sicht auf die Cyber-Sicherheit in Deutschland sollten die verschiedenen Akteure und Institutionen in der Erfüllung ihrer Rollen gestärkt und im Zusammenwirken harmonisiert werden. Auch hierbei wird das fachliche Zusammenspiel der Forschungseinrichtungen, der etablierten Institutionen der öffentlichen Hand, aber vor allem der Wirtschaft selber notwendig sein, um eine substantielle Verbesserung herbeizuführen.

Schaffung eines europäischen Rechtsrahmens
Es sollte ein europäischer Rechtsrahmen geschaffen werden, um den Einsatz und die Vermarktung nicht-europäischer Technologien zu regulieren. Gleichzeitig sollte der ausländische Einfluss auf deutsche und europäische Unternehmen, die sicherheitsrelevante Schlüsseltechnologien entwickeln und der Export dieser Technologien kontrolliert werden. Deutsche und europäische Technologien sollten unter der Berücksichtigung gemeinsamer Mindeststandards an ihre Sicherheit entwickelt werden, um das Vertrauen in sie zu stärken.

Handlungsfeld 3
Intensivierung der Zusammenarbeit von Politik und Wirtschaft

Zusammenarbeit mit der Wirtschaft vertiefen
Politische Akteure sollten die Bedürfnisse der Wirtschaft stärker in den Fokus nehmen und sich nicht gegenüber externen Experten verschließen. Die Politik trägt die Verantwortung, passende Rahmenbedingungen für eine durchweg hohe Cyber-Sicherheit in Deutschland zu schaffen, welche beispielsweise die Entwicklung wichtiger Schlüsseltechnologien durch deutsche beziehungsweise europäische Unternehmen ermöglichen und fördern. Die bestehenden Institutionen und Verbände können die Grundlage bilden, sollten aber auch für Zielgruppen außerhalb der Expertenkreise erweitert werden.

Akteure aus der Wirtschaft und Gesellschaft müssen ihre Belange aktiv in die Politik bringen
Unternehmen, Interessenverbände und gesellschaftliche Akteure haben ebenso die Verantwortung, ihre Belange in geeignetem Rahmen in die Politik einzubringen. Der Bitkom geht mit gutem Beispiel voran und beteiligt sich aktiv an politischen Diskursen. Ein funktionierender und produktiver Austausch zwischen Politik, Gesellschaft, Wirtschaft und Forschung ist dabei elementar. Die Allianz für Cybersicherheit ist beispielsweise eine Initiative, die dafür eine Austauschplattform bereitstellt. Nur so können etwaige Anreizsysteme und Förderprogramme attraktiv gestaltet und die Innovationskraft gestärkt werden.

Handlungsfeld 4
Verhältnismäßige und ausbalancierte Regulierung

Balance in der Regulierung von Cyber-Sicherheitsmaßnahmen finden
Die Befragung zeigt, dass der Fokus bei der Regulierung darauf liegen sollte, welche Bereiche zu regulieren sind. Es ist daher entscheidend, dass die Politik den tatsächlichen Handlungs- und Regulierungsbedarf identifiziert und dann abwägt, ob der angedachte Eingriff auch praktikabel und verhältnismäßig ist. Dafür ist es wichtig, dass Politik und Wirtschaft eng im Austausch stehen und die Gestaltung und Umsetzung dieser Prozesse gemeinsam voranbringen.

Qualität in der Umsetzung von Cyber-Sicherheitsmaßnahmen verbessern
Wichtig ist, dass die Umsetzung von Maßnahmen zur Verbesserung der Cyber-Sicherheit effektiv und schnell geschieht. Hierzu braucht es ein funktionierendes Rahmensystem, das die Bedingungen zur effizienten Implementierung dieser Maßnahmen schafft. Aus der Umfrage geht hervor, dass sich fast drei Viertel der Befragten eine stärkere Zentralisierung bei der Umsetzung wünschen.

Future Foresight Methode

Um zukunftsorientierte, szenarienbasierte Lösungen für eine mögliche Umsetzung von Handlungsempfehlungen zu gestalten, hat Deloitte die Future Foresight[6] Methode entwickelt. Damit verfolgen wir das Ziel, unsere Sicht und unser Verständnis der zukunftsformenden Einflüsse zu erweitern, indem das Gewicht großer Schlagworte und Entwicklungen reduziert wird. Das Modell hilft Entscheidungsträgern dabei, sich auf relevante Faktoren zu fokussieren, welche ihnen ansonsten entgehen könnten. Es bestärkt sie darin, robuste und flexible Entscheidungen zu treffen. Future Foresight ermöglicht eine langfristige Strategieentwicklung. Ausgehend von den treibenden Kräften hinter Entwicklungen werden Trends abgeleitet und mögliche Implikationen betrachtet. Entgegen vieler traditioneller Methoden bezieht Future Foresight die uns umgebende Komplexität mit ein und unterstützt Entscheidungsträger dabei, die dringendsten und komplexesten Fragen anzugehen und zu kontrollieren.

[6] Future Foresight: Understanding today's and tomorrow's driving forces.
https://www.deloitte.com/de/de/pages/risk/articles/future-foresight.html

Ansprechpartner

Peter J. Wirnsperger
Lead Civil Government
Tel: +49 40 32080 4675
pwirnsperger@deloitte.de

Marius von Spreti
Cyber Risk Leader
Tel: +49 89 29036 5999
mvonspreti@deloitte.de

Alle weiteren Ausgaben des Cyber Security Reports finden Sie auf unserer Webseite.

deloitte.com/de/cyber-security-report

Deloitte.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen (zusammen die „Deloitte-Organisation“). DTTL (auch „Deloitte Global“ genannt) und jedes ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL-Mitgliedsunternehmen und verbundene Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen und nicht für die der anderen. DTTL erbringt selbst keine Leistungen gegenüber Mandanten. Weitere Informationen finden Sie unter www.deloitte.com/de/UeberUns.

Deloitte ist ein weltweit führender Dienstleister in den Bereichen Audit und Assurance, Risk Advisory, Steuerberatung, Financial Advisory und Consulting und damit verbundenen Dienstleistungen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Unser weltweites Netzwerk von Mitgliedsgesellschaften und verbundenen Unternehmen in mehr als 150 Ländern (zusammen die „Deloitte-Organisation“) erbringt Leistungen für vier von fünf Fortune Global 500®-Unternehmen. Erfahren Sie mehr darüber, wie rund 330.000 Mitarbeiter von Deloitte das Leitbild „making an impact that matters“ täglich leben: www.deloitte.com/de

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), ihr weltweites Netzwerk von Mitgliedsunternehmen noch deren verbundene Unternehmen (zusammen die „Deloitte-Organisation“) erbringen mit dieser Veröffentlichung eine professionelle Dienstleistung. Diese Veröffentlichung ist nicht geeignet, um geschäftliche oder finanzielle Entscheidungen zu treffen oder Handlungen vorzunehmen. Hierzu sollten Sie sich von einem qualifizierten Berater in Bezug auf den Einzelfall beraten lassen.

Es werden keine (ausdrücklichen oder stillschweigenden) Aussagen, Garantien oder Zusicherungen hinsichtlich der Richtigkeit oder Vollständigkeit der Informationen in dieser Veröffentlichung gemacht, und weder DTTL noch ihre Mitgliedsunternehmen, verbundene Unternehmen, Mitarbeiter oder Bevollmächtigten haften oder sind verantwortlich für Verluste oder Schäden jeglicher Art, die direkt oder indirekt im Zusammenhang mit Personen entstehen, die sich auf diese Veröffentlichung verlassen. DTTL und jede ihrer Mitgliedsunternehmen sowie ihre verbundenen Unternehmen sind rechtlich selbstständige und unabhängige Unternehmen.

Stand 08/2021