Deloitte.

Cyber Security Report 2018

Teil 1: Staat und Wirtschaft – Zusammenwirken bei Digitalisierung und Sicherheit

Vorwort 04

Executive Summary 05

1. Zum Stand der Digitalisierung 06

2. Bedrohung und Schutz 12

    2.1 Einschätzung der Gefährdung 12

    2.2 Gesetzliche Anforderungen 15

3. Zusammenwirken von Staat und Wirtschaft 19

    3.1 Schutz und aktive Cyber-Verteidigung 19

    3.2 Hohe Erwartungen an staatliche Unterstützung 24

Handlungsfelder 28

Ansprechpartner 30

Vorwort

Die Dynamik der Digitalisierung zählt zu den wichtigsten Erfolgsfaktoren für die Wirtschaft in Europa und insbesondere in Deutschland. Digitalisierung kann nur erfolgreich sein, wenn sie mit Cyber Security und Informationssicherheit Hand in Hand geht.

Industrie 4.0, Big-Data-Analysen und künstliche Intelligenz sind wegweisende technologische Treiber der Digitalisierung und die entscheidenden Wirtschaftsfaktoren der Zukunft. Digitalisierung und Cyber- und Informationssicherheit betreffen nicht nur Unternehmen unabhängig von Größe und Branche, sondern auch den Staat und seine Verwaltungsstruktur. Wirtschaftsunternehmen können das Potenzial für ihre Geschäftsmodelle nutzen – der Staat sollte dies unterstützen, indem er einen Ordnungsrahmen schafft, der Rechtssicherheit und die Sicherheit für Unternehmen sowie Bürger gewährleistet und die Effizienz seines Verwaltungshandelns erhöht.

In der öffentlichen Verwaltung und in der privaten Wirtschaft sind zahlreiche Initiativen der Digitalisierung gestartet worden. Intelligente Technologien werden zu einem der größten Innovationstreiber. Sie werden nicht nur die industrielle Produktion revolutionieren, sondern auch Rechtsberatung geben, medizinische Operationen durchführen und unsere Autos fahren. Allerdings könnten uns diese Technologien auch lückenlos überwachen, belohnen und bestrafen sowie für Spionage, Verbrechen und kriegerische Handlungen missbraucht werden. Mit diesen Technologien geht auch eine neue Bedrohungs- und Gefährdungslage einher, die durch adäquate Cyber-Security-Maßnahmen adressiert werden muss.

Wir haben den Fokus der langjährigen Trendstudie mit dem Institut für Demoskopie Allensbach vor dem Hintergrund des beschriebenen umfassenden Zusammenhangs in diesem Jahr um wesentliche neue Themen ergänzt:

Digitalisierung als politisches Ziel
Kann der Staat aus Sicht der Entscheidungsträger dazu beitragen, die Digitalisierung in Deutschland voranzutreiben, und werden hierbei durch die Bundesregierung die richtigen Schwerpunkte gesetzt?

Stand der Digitalisierung in deutschen Unternehmen
Welche Schwerpunkte setzen die Unternehmen in ihren Digitalisierungsstrategien?

Reputationsrisiken und Fake News
Soziale Netzwerke – Chance oder Risiko? Wie gehen Unternehmen mit der Bedrohung um?

Wir haben in dem hier vorliegenden Teil 1 der Studie auf die Digitalisierung und Cyber-Sicherheit auf politischer und gesamtgesellschaftlicher Ebene abgestellt, während Teil 2 die Situation in den Unternehmen beleuchtet.

Executive Summary

Die Ergebnisse der Befragung führen zu den folgenden Kernaussagen:

Digitalisierung und Industrie 4.0
Industrie 4.0, Big Data und künstliche Intelligenz sind in der Industrie unterschiedlich angekommen. Unabhängig von der Branche, aber insbesondere bei den größeren Unternehmen ist Big Data ein Thema, künstliche Intelligenz hingegen ist für die meisten noch nicht von Bedeutung. Die hohe Relevanz der Industrie 4.0 für den Wirtschaftsstandort Deutschland ist erkannt und gerade fertigende Unternehmen sind bei der Vernetzung ihrer Produktionsanlagen auch schon sehr weit fortgeschritten.

Einschätzung der Gefährdung
Auch in diesem Jahr lässt sich feststellen, dass die Wahrnehmung der Gefährdung durch einige der betrachteten Cyber-Risiken gegenüber den Vorjahren gestiegen ist. Computerviren beziehungsweise Schadsoftware werden in diesem Jahr von den Top-Entscheidern als größtes Risiko genannt, dicht gefolgt von Fake News und Datenbetrug im Internet. In der Wahrnehmung von Bedrohungen gehen die Risikoeinschätzungen von Abgeordneten und Wirtschaftsführern auseinander. Dabei sehen Letztere für fast alle Bedrohungsszenarien größere Risiken für die Bürger als Politiker.

Gesetzliche Anforderungen
Auch wenn rund die Hälfte der Wirtschaftsführer davon überzeugt ist, dass für das eigene Unternehmen keine regulatorischen Anforderungen im Bereich IT-Sicherheit existieren, so ist insgesamt das generelle Bewusstsein für gesetzliche Verpflichtungen im Vergleich zum Vorjahr gestiegen.

Staatlicher Schutz und aktive Cyber-Verteidigung
Die kontroverse Debatte um die Frage, ob der Staat eine aktive Cyber-Verteidigung betreiben soll (siehe auch Deloitte European Cyber Defense Report 2018), spiegelt sich in den Ergebnissen der Umfrage wider. So bewerten nicht nur Wirtschaftsführer und Abgeordnete dies unterschiedlich, es gibt außerdem zu dieser Thematik je nach Parteizugehörigkeit stark divergierende Ansichten der einzelnen Politiker.

Hohe Erwartungen an staatliche Unterstützung
Sowohl bei der Digitalisierung, als auch bei der Cyber-Sicherheit wünschen sich die Wirtschaftsführer mehr staatliche Unterstützung. Eine deutliche Mehrheit der Wirtschaftsführer vertritt die Auffassung, dass der Staat den Prozess der Digitalisierung in Deutschland nicht ausreichend unterstützt, selbst zwei Drittel der befragten Politiker sehen das so. Die Schwerpunkte werden mehrheitlich als falsch gesetzt bewertet. Zur Erhöhung der Cyber-Sicherheit werden mehr Informationen über aktuelle Gefährdungen und aktive Unterstützung im Angriffsfall gewünscht.

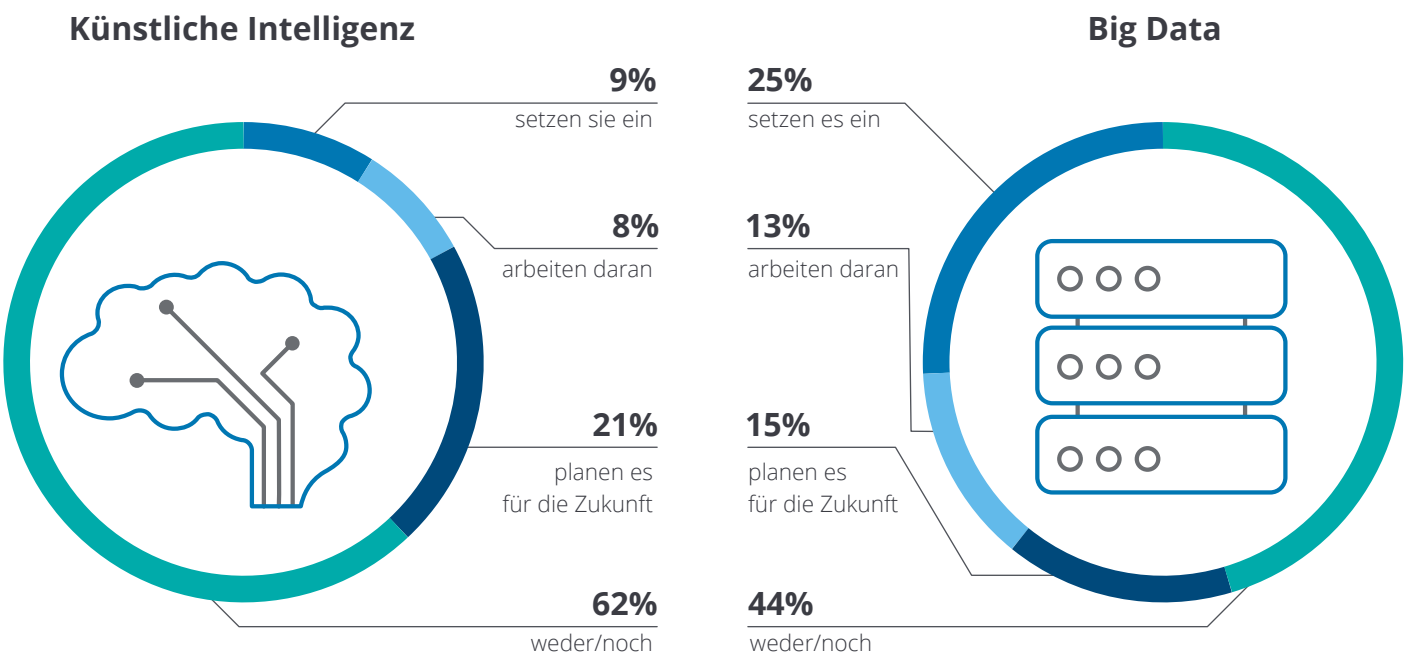
1. Zum Stand der Digitalisierung

In einem Atemzug mit Digitalisierung werden häufig die Schlagworte Industrie 4.0, Big Data oder künstliche Intelligenz (KI) genannt. Im Rahmen dieser Studie wurden die Teilnehmer aus der Wirtschaft befragt, welche Rolle diese Begriffe in ihrer Unternehmensrealität spielen und was sie damit verbinden.

Zunächst einmal ist festzuhalten, dass Big Data, KI und Industrie 4.0 bis dato sehr unterschiedlich in der Unternehmensrealität angekommen sind.

Big Data, also die automatisierte Analyse großer Datenmengen, ist für die Mehrheit der mittleren und großen Unternehmen ein Thema. Ein Viertel der Umfrageteilnehmer aus der Wirtschaft insgesamt setzt solche Verfahren bereits ein, weitere 13 Prozent arbeiten daran, und 15 Prozent planen es für die Zukunft.

Abb. 1 – Stand der Digitalisierung in den Unternehmen



Antworten mit „weiß nicht, keine Angabe“ sind nicht abgebildet.

Big Data ist für die Mehrheit der Unternehmen bereits ein Thema.

Methoden der künstlichen Intelligenz bei Geschäfts- oder Produktionsanwendungen einzusetzen, ist hingegen für die meisten Unternehmen derzeit kein Thema. Lediglich 9 Prozent setzen hier bereits auf KI-Lösungen, weitere 8 Prozent arbeiten daran, und 21 Prozent planen das für die Zukunft. Für 62 Prozent jedoch spielt das Thema derzeit keine Rolle.

Die Politik sieht KI als einen zentralen Treiber der Digitalisierung. Im September 2018 hat sich die Enquete-Kommission „künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale" des Deutschen Bundestags konstituiert. In dem Gremium aus 19 Bundestagsabgeordneten und 19 externen Sachverständigen sollen bis zum Sommer 2020 Handlungsempfehlungen im Umgang mit künstlicher Intelligenz entwickelt werden. Der Bundestagspräsident betonte bei der konstituierenden Sitzung, die Dynamik der Digitalisierung habe mit der Forschung zur KI eine neue Dimension erreicht, es sei deshalb wichtig festzustellen, was KI bedeute, was sie leisten könne sowie welche Chancen und Herausforderungen für Staat, Gesellschaft und Recht sie darstelle. Das münde in die Frage, wie diese Entwicklung gestaltet und sichergestellt werden könne.[1]

Weiterhin hat das Bundeskabinett im Juli 2018 die Eckpunkte für eine Strategie künstliche Intelligenz der Bundesregierung beschlossen. Damit sollen Forschung, Entwicklung und Nutzung in Deutschland an die Weltspitze gebracht werden. Hierbei sollen die verantwortungsvolle Anwendung, die dem Wohl der Gesellschaft dient, und die Erschließung von Wertschöpfungspotenzialen im Vordergrund stehen. Dazu soll die Forschungslandschaft in Deutschland ausgebaut und innerhalb Europas vernetzt werden. Bei der Identifizierung menschenzentrierter Anwendungen soll die Zusammenarbeit und nicht die Konkurrenz von Mensch und Maschine fokussiert werden.

Das Thema künstliche Intelligenz ist aktuell bei den wenigsten Unternehmen auf der Agenda.

Für Politik und Wirtschaft ist Industrie 4.0 ein zentrales Thema – von der Bevölkerung wird die Bedeutung des Themas jedoch eher unterschätzt.

Industrie 4.0 jedoch misst die Mehrheit der befragten Führungskräfte eine große Bedeutung zu. Von den Entscheidungsträgern in Unternehmen sind 61 Prozent davon überzeugt, dass das Projekt Industrie 4.0 für den Wirtschaftsstandort Deutschland sehr wichtig ist. Abgeordnete stehen sogar zu 82 Prozent auf diesem Standpunkt. Weitere 36 beziehungsweise 15 Prozent halten es zumindest für wichtig.

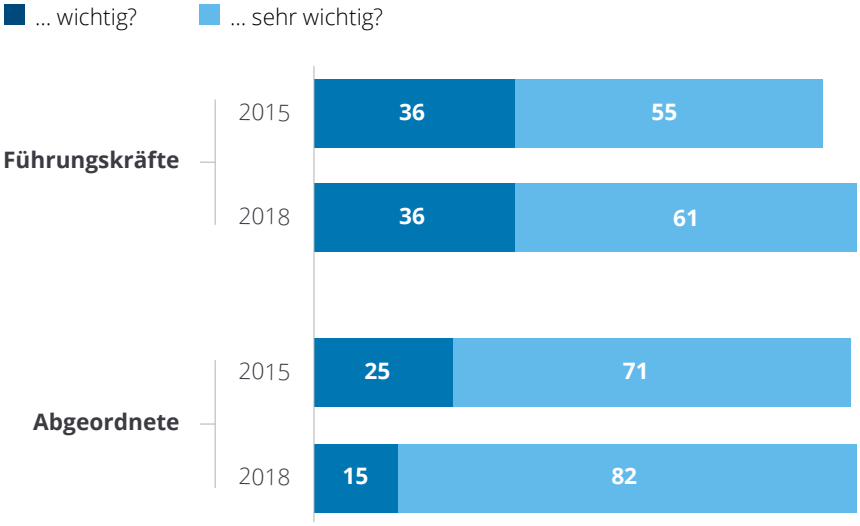
Für Politik und Wirtschaft ist Industrie 4.0 ein zentrales Thema. Von der Bevölkerung wird dessen Bedeutung jedoch eher unterschätzt: So waren im vergangenen Jahr lediglich 18 Prozent der Bevölkerung davon überzeugt, dass es wichtig ist, die Digitalisierung voranzutreiben, um Deutschland voranzubringen und dem Land eine gute Zukunft zu sichern. Von 20 adäquaten Maßnahmen belegte die Digitalisierung damit nur den vorletzten Platz.[2]

[1] Deutscher Bundestag, Enquete-Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale".
[2] Allensbacher Archiv, IfD-Umfrage 7286, Februar/März 2017.

In der Wirtschaft und bei Politikern wird die Wichtigkeit des Themas als höher wahrgenommen. Im Vergleich zu 2015 ist die Bedeutung von Industrie 4.0 für die Digitalisierung der Wirtschaft Deutschlands aus Sicht der Entscheider gestiegen. Vor drei Jahren waren „nur“ 55 Prozent der Wirtschaftsführer und 71 Prozent der Abgeordneten der Überzeugung, dass das Projekt Industrie 4.0 für den Wirtschaftsstandort Deutschland sehr wichtig ist.

Abb. 2 – Wahrgenommene Bedeutung von Industrie 4.0 ist gewachsen

Halten Sie das Projekt Industrie 4.0 für den Wirtschaftsstandort Deutschland für ...

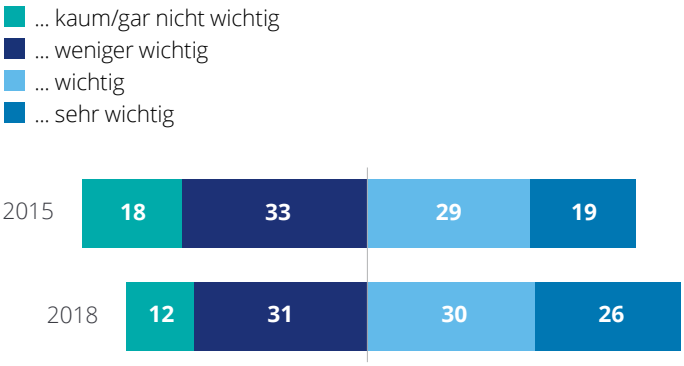


In Prozent der Nennungen

Die Bedeutung von Industrie 4.0 für das eigene Unternehmen veranschlagen Wirtschaftsführer ebenfalls als hoch, allerdings nicht so hoch wie für den Wirtschaftsstandort insgesamt. Insbesondere im produzierenden Gewerbe ist die wahrgenommene Bedeutung für das eigene Unternehmen im Vergleich zu 2015 aber deutlich gestiegen. Von den Wirtschaftsführern insgesamt halten aktuell 26 Prozent das Projekt Industrie 4.0 für die Zukunft des eigenen Unternehmens für sehr wichtig, weitere 30 Prozent für wichtig.

Abb. 3 – Zunehmende Bedeutung von Industrie 4.0 auch für das eigene Unternehmen

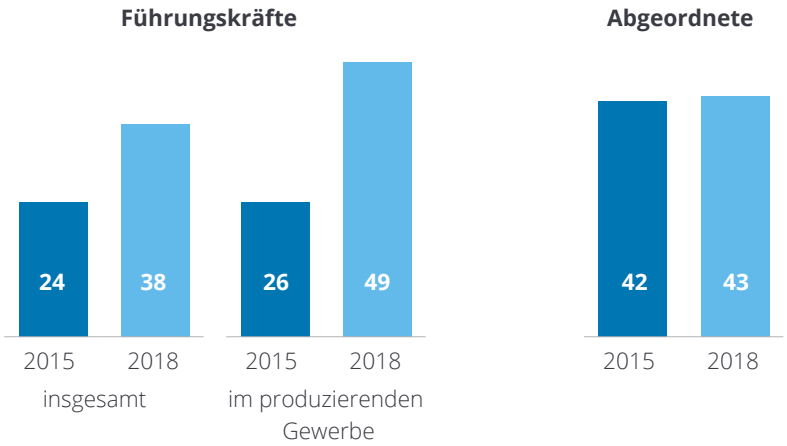
Führungskräfte in Unternehmen sagen, für die Zukunft des eigenen Unternehmens ist Industrie 4.0 ...



In Prozent der Nennungen

Abb. 4 – Intensivere Auseinandersetzung mit Industrie 4.0 in der Wirtschaft

Es haben sich schon (sehr) intensiv mit dem Thema Industrie 4.0 beschäftigt …

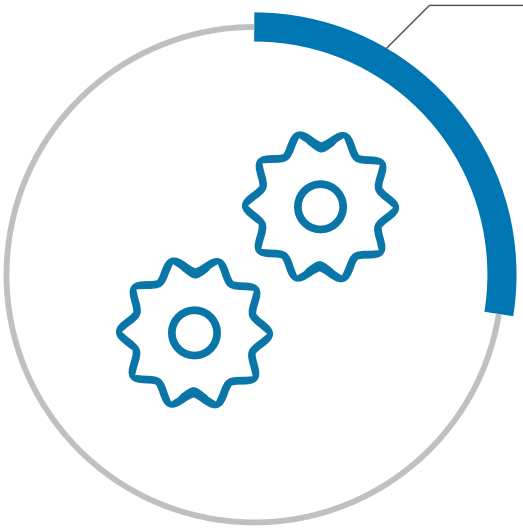


In Prozent der Nennungen

Die Bedeutung von Industrie 4.0 für das eigene Unternehmen veranschlagen Wirtschaftsführer ebenfalls als hoch, allerdings nicht so hoch wie für den Wirtschaftsstandort insgesamt.

2018 geben nur 38 Prozent der Führungskräfte an, sich bereits intensiver mit Industrie 4.0 beschäftigt zu haben. Zwar ist gegenüber 2015 der Anteil der Wirtschaftsführer, der sich mit dem Thema schon intensiv oder sogar sehr intensiv auseinandersetzte, deutlich gestiegen, dennoch erklärt dieses nach wie vor bemerkenswert niedrige Niveau warum auf eine entsprechende offene Frage ein hoher Anteil nur sehr allgemeine – wenn überhaupt zutreffende – Beschreibungen dessen gibt, was unter Industrie 4.0 zu verstehen ist. So nennen 41 Prozent lediglich das Stichwort „Digitalisierung“ oder verwandte Begriffe, 38 Prozent die Vernetzung von zum Beispiel Maschinen oder Produktionsanlagen. Die Veränderung von Produktionsabläufen, zum Beispiel durch Flexibilisierung der Fertigung, Individualisierung von Produkten, Dezentralisierung und zunehmende Automatisierung nennen 13 Prozent, die Selbststeuerung von Maschinen beziehungsweise dass Maschinen untereinander kommunizieren, 10 Prozent.

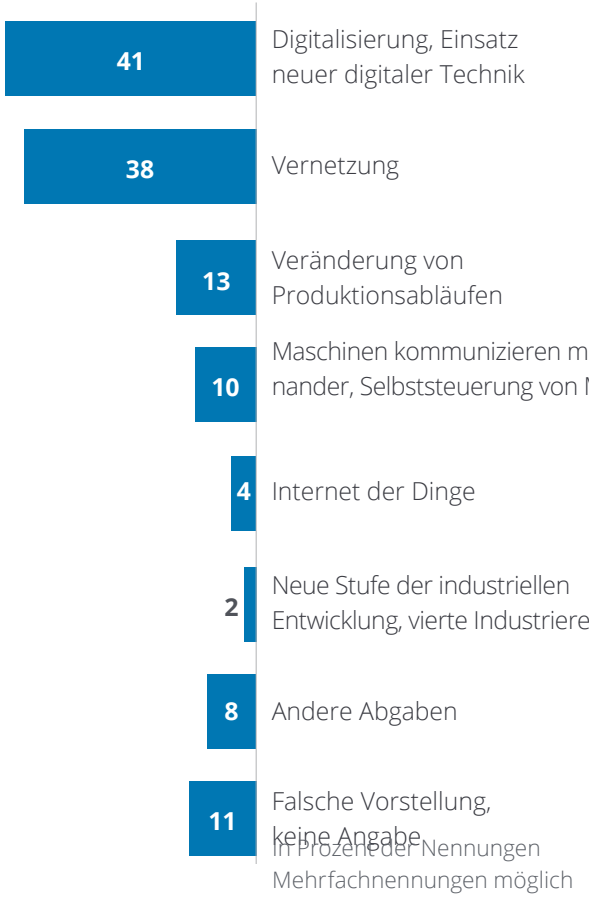
Abb. 5 – Was Top-Führungskräfte unter Industrie 4.0 verstehen



38%

der Führungskräfte in Unternehmen haben sich schon (sehr) intensiv mit Industrie 4.0 beschäftigt, im produzierenden Gewerbe ist es fast die Hälfte.

Von allen befragten Führungskräften verstehen unter Industrie 4.0 ...



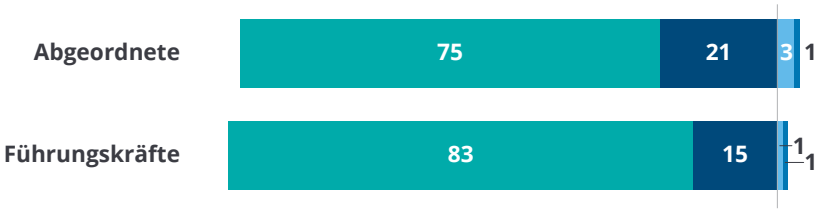
Gleichzeitig ist die Vernetzung von Produktionsanlagen bereits weit fortgeschritten. In insgesamt 45 Prozent der Unternehmen sind die Produktionsanlagen bereits untereinander oder mit Büroanwendungen vernetzt, weitere 8 Prozent arbeiten konkret an einer solchen Vernetzung und 9 Prozent planen das für die Zukunft.

Erst 38 Prozent der Führungskräfte haben sich intensiver mit Industrie 4.0 beschäftigt, haben aber ein unterschiedliches Verständnis davon.

Abb. 6 – Steigendes Risiko durch Industrie 4.0

Mit Industrie 4.0 wird das Risiko von Cyber-Angriffen auf Unternehmen ...

- ... steigen
- ... da wird sich nicht viel ändern
- ... sinken
- ... schwer zu sagen/keine Angaben



In Prozent der Nennungen

Dass das Risiko von Cyber-Angriffen mit der Umsetzung von Industrie 4.0 und der Vernetzung von Produktionsprozessen steigt, darin sind sich die Führungskräfte und Abgeordneten weitgehend einig. Über 80 Prozent der Wirtschaftsführer teilen diese Einschätzung. Abgeordnete sehen dies zu drei Vierteln so. Hier sind wir wieder bei der Ausgangsfrage angelangt und der Bestätigung der Einschätzung, dass Cyber-Sicherheit eine Voraussetzung für das erfolgreiche Gelingen der Digitalisierung ist.

Industrie 4.0 hat in der Wahrnehmung von Wirtschaftsvertretern und Politik eine große und wachsende Bedeutung für den Wirtschaftsstandort Deutschland. Gerade in größeren Unternehmen und der fertigenden Industrie wird die Vernetzung von Produktionsanlagen auch vermehrt eingesetzt. Vor diesem Hintergrund besteht bei vielen Führungskräften jedoch noch Nachholbedarf bezüglich ihres Wissens über die Thematik. Es lässt sich festhalten, dass die komplette Vernetzung von Produktionsanlagen, Büroanwendungen und Warenwirtschaftssystemen die Angreifbarkeit erhöht und besonderen Schutzes bedarf. Dies bedeutet auch mehr Sensibilität im Umgang mit Daten, Schnittstellen und Zugängen. Der Einschätzung der Gefährdung bei gleichzeitig als hoch wahrgenommener Bedeutung von Industrie 4.0 sollte Rechnung getragen werden: Wirtschaftsführer müssen sich intensiver mit dem Thema befassen. Es gilt, sowohl besser mit Risiken umzugehen als auch Chancen besser zu sehen und zu vermitteln.

Durch Industrie 4.0 wird ein höheres Risiko für Cyber-Angriffe befürchtet.

2. Bedrohungen und Schutz

2.1 Einschätzung der Gefährdung

Auch in diesem Jahr lässt sich feststellen, dass die Wahrnehmung der Gefährdung durch einige der betrachteten Cyber-Risiken gegenüber den Vorjahren gestiegen ist.

Viele Cyber-Risiken werden von jeweils deutlichen Mehrheiten der Entscheidungsträger aus Wirtschaft und Politik als großes Risiko für die Menschen in Deutschland eingestuft. Das gilt sowohl für individuelle Risiken wie Computerviren oder Datenbetrug im Internet als auch für kollektive Risiken wie den Ausfall wichtiger Infrastruktureinrichtungen durch Cyber-Angriffe oder eine Manipulation der öffentlichen Meinung durch Fake News.

Dabei sehen Wirtschaftsführer für fast alle Bedrohungsszenarien größere Risiken für die Bürger als Abgeordnete. Besonders deutlich sind diese Unterschiede, wenn es um die Gefahren durch Computerviren beziehungsweise Schadsoftware, um den Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken und die Bedrohung der Privatsphäre durch die zunehmende Vernetzung von Haustechnik und Haushaltsgeräten geht.

Computerviren beziehungsweise Schadsoftware werden in diesem Jahr von den Top-Entscheidern als größtes Risiko wahrgenommen. Der Anteil der Führungskräfte, die darin ein großes Risiko sehen, ist seit 2013 kontinuierlich von 57 Prozent auf aktuell 77 Prozent gestiegen. Das Bundesamt für Sicherheit in der Informationstechnik untermauert die Wahrnehmung mit der Feststellung, dass im Jahr 2018 mehr als 800.000.000 Schadprogramme im Umlauf sind.[3]

Die Wahrnehmung, dass die Manipulation der öffentlichen Meinung durch Fake News ein großes Risiko darstellt, ist seit unserem letzten Bericht 2017 deutlich von 67 auf 75 Prozent der Befragten gestiegen. Der Trend dieser Wahrnehmung lässt sich auch daraus ableiten, dass negative Berichterstattungen und Imageschäden Deliktstypen sind, die in den letzten zwei Jahren die größte Schadenssumme für deutsche Unternehmen mit sich brachten.[4]

Jeweils rund drei Viertel der Top-Entscheider halten Computerviren beziehungsweise Schadsoftware, Datenbetrug im Internet sowie die Manipulation der öffentlichen Meinung durch gefälschte oder irreführende Nachrichten für ein großes Risiko für die Menschen in Deutschland.

[3] BSI, Die Lage der IT-Sicherheit in Deutschland 2018.
[4] Bitkom Research, Wirtschaftsschutz in der Industrie; 8,8 Mrd. EUR in den letzten zwei Jahren.

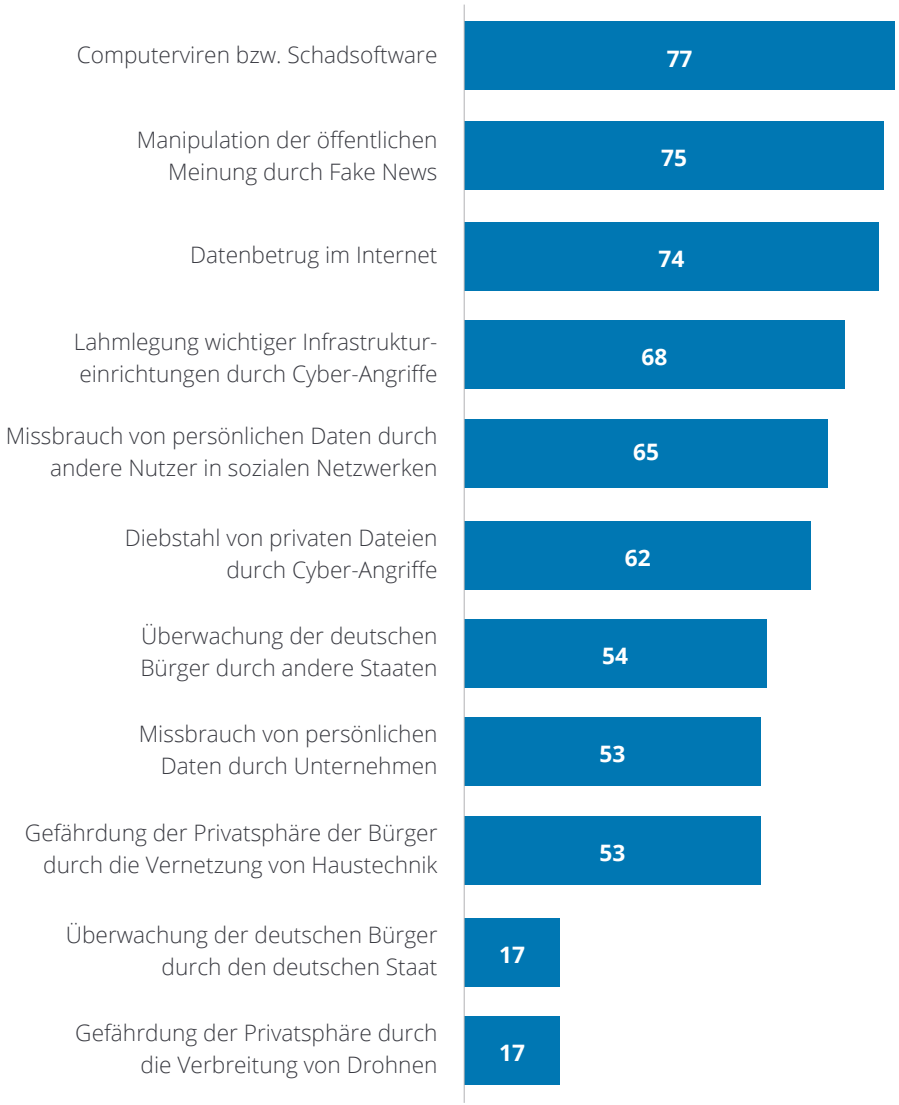
Auch sind Wirtschaftsführer und Abgeordnete derzeit so häufig wie in keiner der vorangegangenen Befragungswellen davon überzeugt, dass von möglichem Datenbetrug im Internet eine große Gefahr für die Bürger im Land ausgeht.

Zwei Drittel der Befragten beurteilen den Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken, den Diebstahl von privaten Dateien und Informationen durch Cyber-Angriffe sowie die Gefahr, dass durch Letztere wichtige Infrastruktureinrichtungen wie Stromnetze oder Krankenhäuser lahmgelegt werden, ebenfalls als großes Risiko. Dieses Risiko sehen Wirtschaftsführer tendenziell häufiger als Abgeordnete – 69 Prozent im Vergleich zu 62 Prozent.

Rund die Hälfte der Wirtschaftsführer und Abgeordneten sieht ein großes Risiko für Bürger durch den Missbrauch beziehungsweise die unerlaubte Weitergabe von persönlichen Daten durch Unternehmen.

Aktuell schätzen 58 Prozent der Wirtschaftsführer, aber „nur" 40 Prozent der Abgeordneten das Risiko, das für die Menschen in Deutschland von einer möglichen Überwachung durch andere Staaten ausgeht, als groß ein. Gegenüber 2017 ist der Unterschied in den Anteilen damit von zehn auf 18 Prozentpunkte gewachsen. Dass der deutsche Staat seine Bürger zu sehr überwacht, halten dagegen „nur" 17 Prozent der Top-Führungskräfte für ein großes Risiko für die Menschen in Deutschland.

Abb. 7 – Wahrgenommene Cyber-Risiken für die Bevölkerung



In Prozent der Nennungen

Die Manipulation der öffentlichen Meinung durch Fake News wird in zunehmendem Maße als großes Risiko eingestuft.

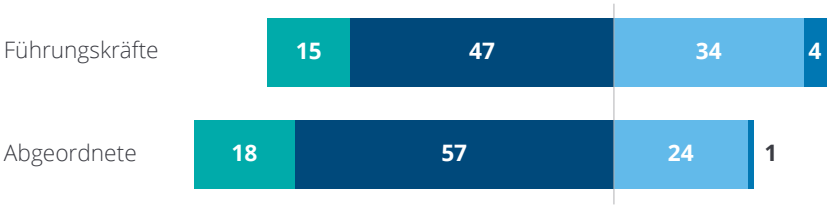
Abb. 8 – Nur eine Minderheit ist überzeugt, dass Deutschland gut vorbereitet ist

Schutz gegen Cyber-Angriffe

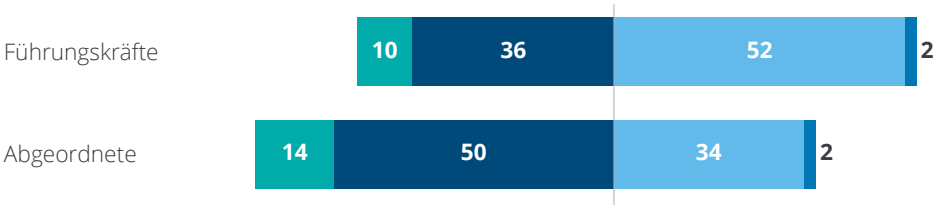
Führungskräfte sehen Deutschland auf Cyber-Angriffe schlechter vorbereitet als Abgeordnete.

- Unentschieden/keine Angaben
- Zweifel
- Einigermaßen vorbereitet
- So gut wie möglich vorbereitet

Cyber-Angriffe auf staatliche Stellen



Cyber-Angriffe auf die Infrastruktur



In Prozent der Nennungen

Zum Stand der Vorbereitung auf mögliche Angriffe auf die Infrastruktur und staatliche Stellen bestehen weiterhin verbreitet Zweifel. Insbesondere beim Schutz der Infrastruktur sind Wirtschaftsführer deutlich skeptischer als Abgeordnete.

Für die befragten Wirtschaftsführer gehören Cyber-Angriffe mittlerweile zum Alltag im Unternehmen. Insgesamt 93 Prozent der mittleren und großen Unternehmen waren bereits IT-Angriffen ausgesetzt, durch die das Unternehmen ausspioniert oder geschädigt werden sollte. 25 Prozent berichten von täglichen Angriffen, weitere 21 Prozent haben ein- oder mehrmals pro Woche damit zu kämpfen, 7 Prozent mehrmals im Monat. Gemäß des Branchenverbands Bitkom erleidet fast die Hälfte der Unternehmen dadurch auch Schäden.[5]

Dieser Hintergrund führt augenscheinlich zu einer kritischen Risikoeinschätzung bei den Wirtschaftsführern im Vergleich zu den Abgeordneten.

[5] Bitkom Research, Wirtschaftsschutz in der Industrie; digitale IT-Angriffe haben bei 47% der Industrieunternehmen einen Schaden verursacht.

2.2 Gesetzliche Anforderungen

Regulatorische Anforderungen erfordern zum Teil umfassende Anpassungen in Unternehmen. So hat beispielsweise die umfangreiche Datenschutz-Grundverordnung (DSGVO) der Europäischen Union, die ab Mai 2018 in Kraft getreten ist, dies wieder eindrucksvoll gezeigt. Vor diesem Hintergrund ist es interessant zu sehen, dass rund die Hälfte der Führungskräfte überzeugt ist, dass für das eigene Unternehmen keine gesetzlichen beziehungsweise regulatorischen Anforderungen im Bereich IT-Sicherheit existieren.

Insgesamt ist – sicherlich auch vor dem Hintergrund der DSGVO-Umsetzung – das Bewusstsein der Führungskräfte für solche Regelungen im Vergleich zum Vorjahresbericht jedoch deutlich gestiegen. 2017 waren lediglich 37 Prozent der Führungskräfte überzeugt, ihr Unternehmen unterliege entsprechenden Anforderungen. Aktuell liegt der Anteil elf Prozentpunkte höher.

Die Mehrheit sowohl der Abgeordneten als auch der Wirtschaftsführer hat Zweifel an der Angemessenheit der Ausstattung staatlicher Stellen hinsichtlich der für die Aufgaben erforderlichen hohen Fachkompetenz, zum Beispiel wenn es um die Schaffung gesetzlicher Rahmenbedingungen bei der IT-Sicherheit geht. Nur knapp ein Drittel der Abgeordneten und knapp jeder fünfte Wirtschaftsführer ist überzeugt, dass in Politik und Verwaltung ausreichend Fachkompetenz in diesem Bereich vorhanden ist. Gut zwei Drittel der Abgeordneten und 79 Prozent der Top-Entscheider aus Unternehmen haben daran ausdrücklich Zweifel. Diese Beurteilungen haben sich im Vergleich zum Vorjahr nur wenig verändert, drücken in der Tendenz eher noch mehr Skepsis aus.

Abb. 9 – Fachkompetenz für gesetzliche Rahmenbedingungen

Verbreitet Zweifel an der Angemessenheit der Ausstattung staatlicher Stellen für die Schaffung gesetzlicher Rahmenbedingungen bei der IT-Sicherheit

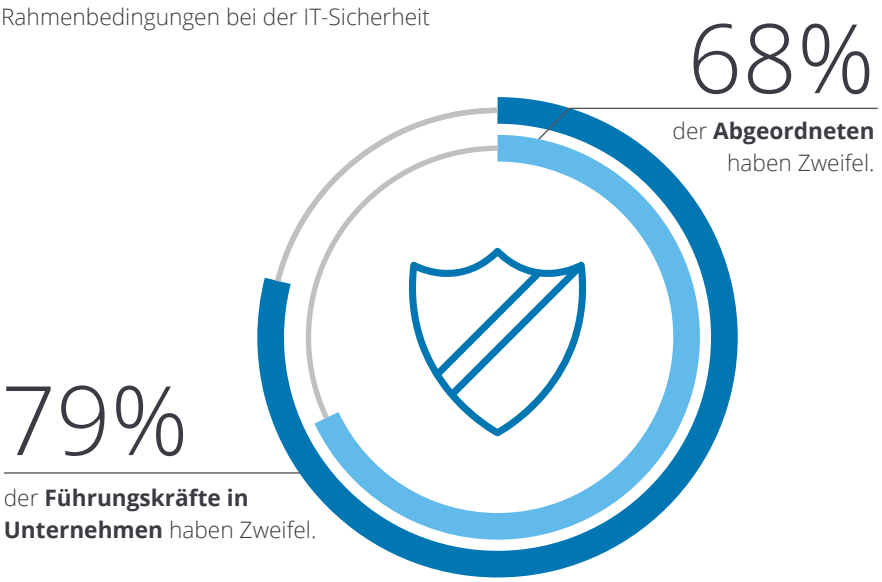
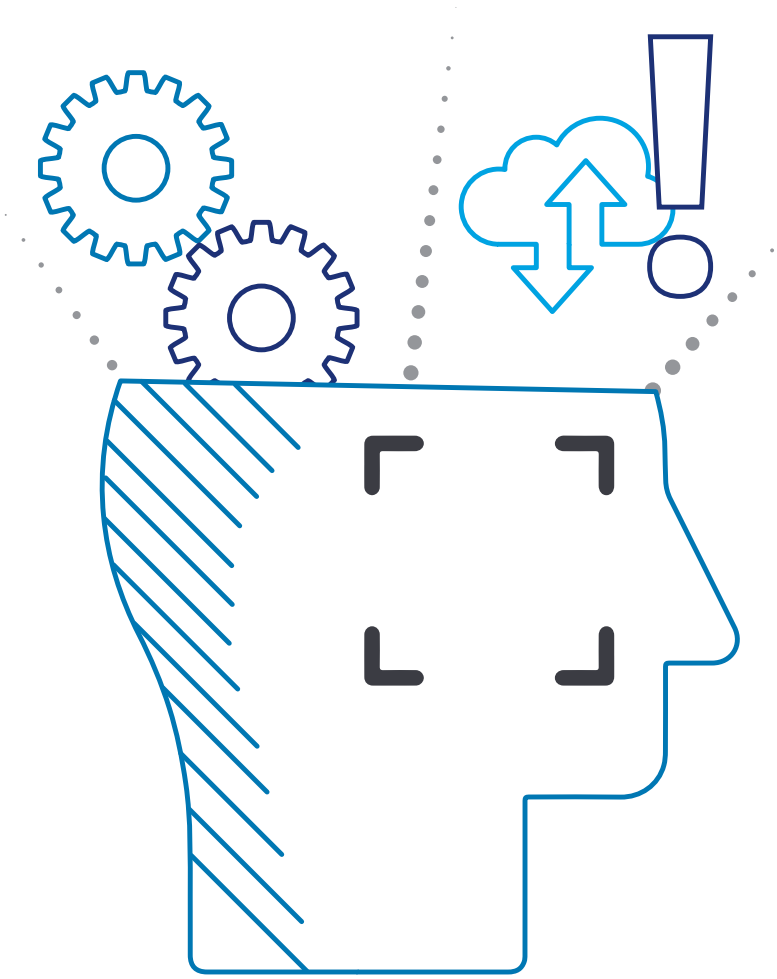


Abb. 10 – Gesetzliche Anforderungen

Rund die Hälfte der Führungskräfte ist überzeugt: Es gibt keine gesetzlichen bzw. regulatorischen Anforderungen im Bereich IT-Sicherheit für das eigene Unternehmen.



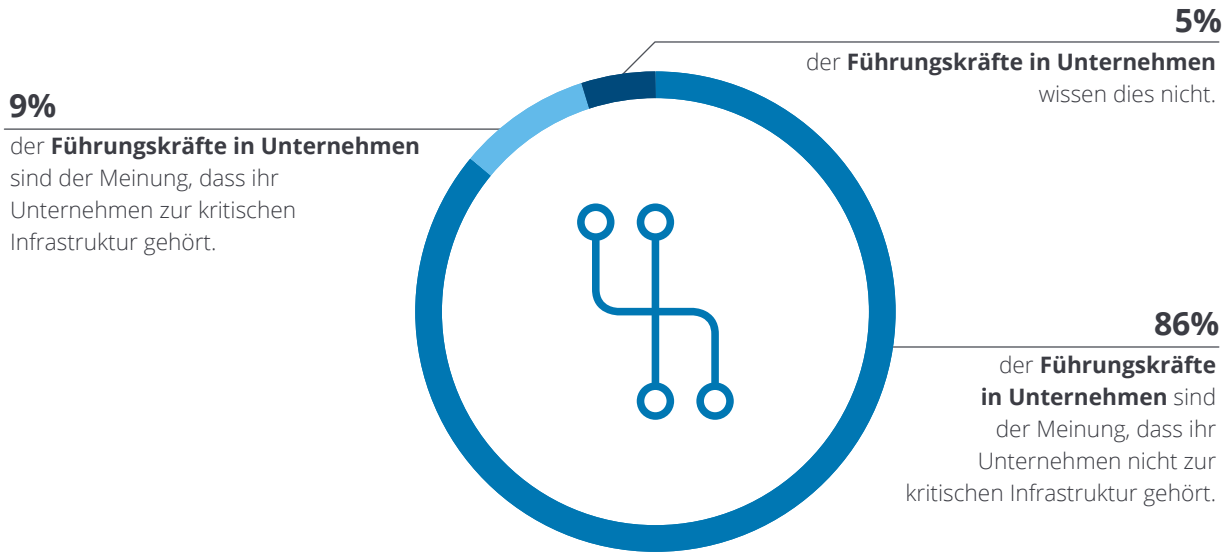
Mit dem seit Juli 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) bestehen in Deutschland gesetzliche Mindestanforderungen an die IT-Sicherheit sogenannter kritischer Infrastrukturen (KRITIS), wie etwa Strom- und Wasserversorgung, Finanzen oder Ernährung. Außerdem wurden auch die Anforderungen für Betreiber digitaler Dienste und Telekommunikationsunternehmen verschärft. Die europäische Grundlage für diese regulatorischen Erweiterungen bildet die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie). Nach dieser sind die europäischen Mitgliedstaaten seit 2016 verpflichtet, ein hohes Maß an Netzwerk- und Informationssicherheit zu gewährleisten.

Die KRITIS-Strategie der Bunderegierung definiert kritische Infrastrukturen als Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Darunter zählen Organisationen und Einrichtungen aus den Bereichen Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur.[6]

Damit zusammenhängend sind dann auch die regulatorischen und gesetzlichen Verpflichtungen um einiges höher für Unternehmen, die mit dem Label KRITIS gekennzeichnet sind. Von den befragten Führungskräften gehen jedoch nur 9 Prozent davon aus, dass ihr Unternehmen zu den KRITIS gehört. Das lässt den Schluss zu, dass die KRITIS-Organisationen und -Einrichtungen in der Gesamtwirtschaft einen zahlenmäßig geringen Teil der deutschen Unternehmen darstellen.

Abb. 11 – Kritische Infrastruktur und gesetzliche Anforderungen

Führungskräfte in Unternehmen sind mehrheitlich davon überzeugt, das eigene Unternehmen gehöre nicht zur kritischen Infrastruktur.



[6] Gemäß Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik.

„Der Staat muss mit den Angreifern Schritt halten können, dazu braucht es auch die Fähigkeit und die Befugnisse zu einer aktiven Cyber-Abwehr.“

Katrin Rohmann, Government & Public Services Industry Leader

„Es gibt noch deutlichen Handlungsbedarf, um Cyber-Sicherheit in Deutschland ganzheitlich gut aufzustellen und der Kritikalität von Cyber-Bedrohungslagen einheitlich bewusst zu werden.“

Peter J. Wirnsperger, Cyber Risk Leader

3. Zusammenwirken von Staat und Wirtschaft

3.1 Schutz & aktive Cyber-Verteidigung

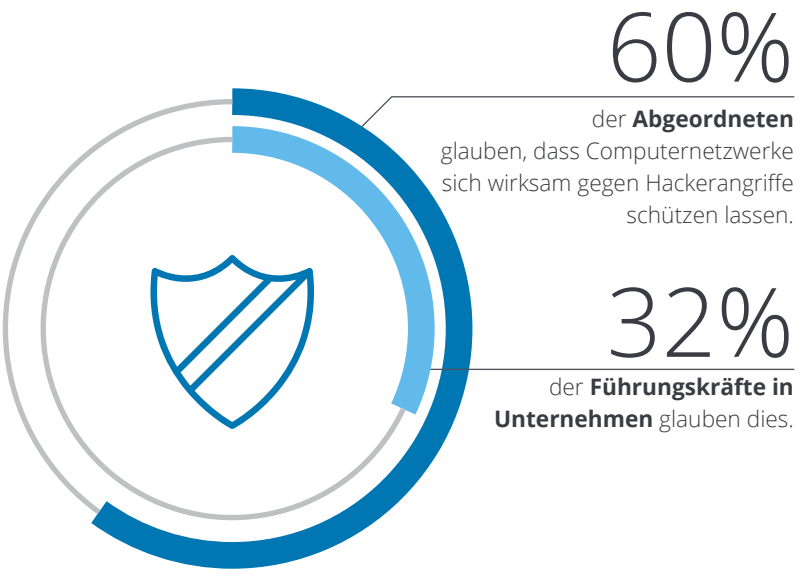
Hackerangriffe betreffen Staaten, Beispiele sind die Angriffe auf Bundesbehörden im Jahr 2017, und Unternehmen, zum Beispiel der Angriff auf RWE im September 2018, gleichermaßen. Mögliche Urheber verüben diese aus unterschiedlichen Intentionen, aus kriminellen Motiven oder zum Zwecke von (Wirtschafts-)Spionage. Die Frage, ob es einen wirksamen Schutz gegen Hackerangriffe gibt, wird kontrovers in Gesellschaft, Politik und Wirtschaft diskutiert. Vor diesem Hintergrund gehen auch die Einschätzungen von Abgeordneten und Führungskräften aus der Wirtschaft in dieser Frage deutlich auseinander: Während eine deutliche Mehrheit der Politiker der Überzeugung ist, ein wirksamer Schutz ist möglich, halten rund zwei Drittel der Unternehmenslenker einen wirksamen Schutz nicht für möglich. Im Vergleich zum Vorjahr sind diese Einschätzungen fast unverändert, tendenziell zeigen sich Führungskräfte aus der Wirtschaft noch etwas skeptischer, was die Möglichkeit eines wirksamen Schutzes von Computernetzwerken vor Hackerangriffen angeht, als im vorjährigen Bericht.

Wirtschaftsvertreter haben augenscheinlich die Erfahrung gemacht, dass aufgrund der Bedrohungsszenarien ein umfassender Schutz wirtschaftlich und technisch nicht darstellbar ist. Daher nehmen die Bemühungen zu, neben reinen Schutzmaßnahmen auch die Resilienz von Organisationen und Einrichtungen zu stärken.

Organisatorische Resilienz bedingt die Fähigkeit, Bedrohungen zu antizipieren, sich auf mögliche Angriffe vorzubereiten, die schädlichen Auswirkungen von Angriffen zu minimieren und zu tolerieren, um schließlich die Geschäftstätigkeiten möglichst schnell wieder aufnehmen zu können und gegebenenfalls die eigenen Sicherheitsmaßnahmen anzupassen.

Abb. 12 – Gibt es wirksamen Schutz gegen Hackerangriffe? Gegensätzliche Einschätzungen von Politikern und Wirtschaftsführern

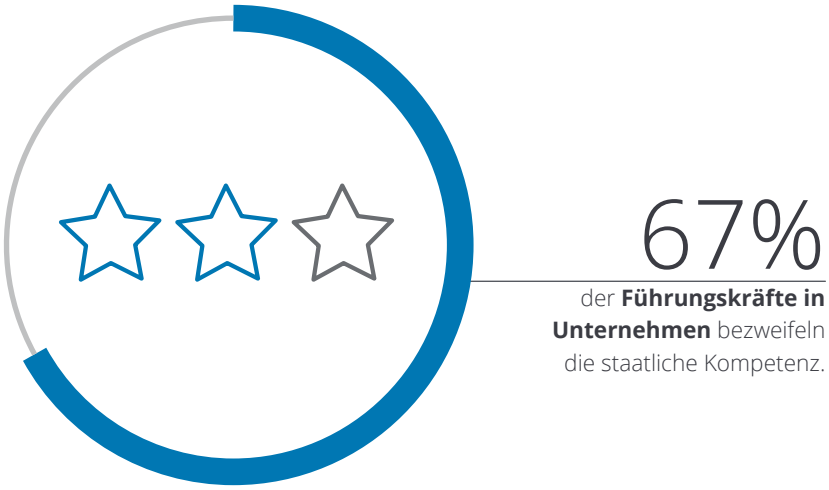
Abgeordnete und Führungskräfte schätzen den möglichen Schutz gegen Hackerangriffe unterschiedlich ein.



„Viele Unternehmen haben eine permanente Gefährdung durch Cyber-Risiken erkannt. Dabei haben sie aber auch die Erfahrung gemacht, dass ein 100%iger Schutz im Sinne einer reinen Abwehr wirtschaftlich und technisch nicht darstellbar ist. Sie setzen zunehmend auf Maßnahmen, die die Resilienz ihrer Unternehmen ganzheitlich erhöhen. Das stellt einen umfassenderen Ansatz dar."

Peter J. Wirnsperger, Cyber Risk Leader

Abb. 13 – Zweifel an der Fachkompetenz in staatlichen Stellen für die Abwehr von Cyber-Angriffen



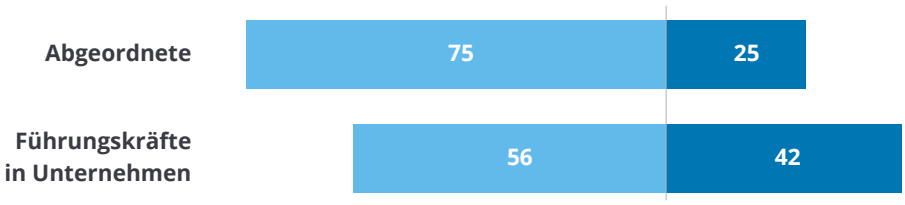
Vorfälle wie der oben beschriebene Hackerangriff auf die Bundesbehörden und die wiederholten Cyber-Attacken auf den Deutschen Bundestag seit 2015 oder auch die Errichtung neuer Cyber-Kapazitäten im Kontext der Bundeswehr haben vermehrt die Frage auf die Agenda gebracht, ob diese Einrichtungen über die notwendigen Kompetenzen für die Abwehr von Cyber-Angriffen verfügen. Doch sowohl bei Wirtschaftsführern als auch bei Abgeordneten bestehen Zweifel an der Kompetenz der staatlichen Stellen, die für den Schutz vor Cyber-Angriffen zuständig sind. Nur 31 Prozent der Abgeordneten und 26 Prozent der Wirtschaftsführer glauben, dass dort ausreichend Fachkompetenz verfügbar ist, jeweils rund zwei Drittel äußern daran ausdrücklich Zweifel.

Abb. 14 – Kann der Staat Unternehmen wirkungsvoll beim Schutz vor Cyber-Angriffen unterstützen?

Staatliche Unterstützung

Vertrauen in die Möglichkeit staatlicher Unterstützung bei Abgeordneten stärker als in der Wirtschaft.

- Der Staat kann nicht viel tun.
- Wirkungsvolle Unterstützung möglich.



In Prozent der Nennungen

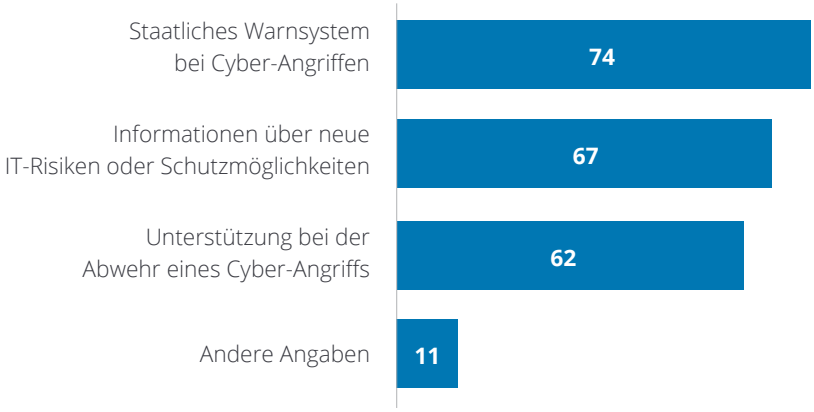
Eine wirkungsvolle Unterstützung von Unternehmen durch den Staat beim Schutz vor IT-Angriffen hält jedoch eine Mehrheit von 56 Prozent der Entscheider aus der Wirtschaft für möglich. Abgeordnete trauen das dem deutschen Staat sogar zu 75 Prozent zu. Dennoch bleibt eine starke Minderheit der Wirtschaftsführer auch hier skeptisch (42%). Im Vergleich zum Vorjahr ist die Überzeugung, der Staat kann Unternehmen hier wirkungsvoll unterstützen, bei den Abgeordneten deutlich gewachsen (2017: 61%), die Einschätzungen der Wirtschaftsführer haben sich dagegen nur marginal verändert.

Wie könnte eine solche Unterstützung aussehen? Von denjenigen Entscheidern, die die Möglichkeit einer wirkungsvollen Unterstützung von Unternehmen durch den Staat bei der Abwehr von IT-Angriffen sehen, würden rund drei Viertel ein staatliches Warnsystem vor Cyber-Angriffen für ein gutes Instrument halten. Daneben meinen 62 Prozent, eine unmittelbare Unterstützung von Unternehmen bei der Abwehr von Cyber-Angriffen wäre sinnvoll. Eine andere Unterstützungsform wäre hierbei, dass der Staat Unternehmen über neue IT-Risiken und Schutzmöglichkeiten auf dem Laufenden hält; dies wird von ca. zwei Dritteln gutgeheißen.

Abb. 15 – Unterstützung ist auf mehreren Ebenen sinnvoll

Schutz vor Cyber-Angriffen

Wenn eine wirkungsvolle Unterstützung durch den Staat für möglich erachtet wird, sollte sie sich auf folgende Bereiche beziehen:



In Prozent der Nennungen

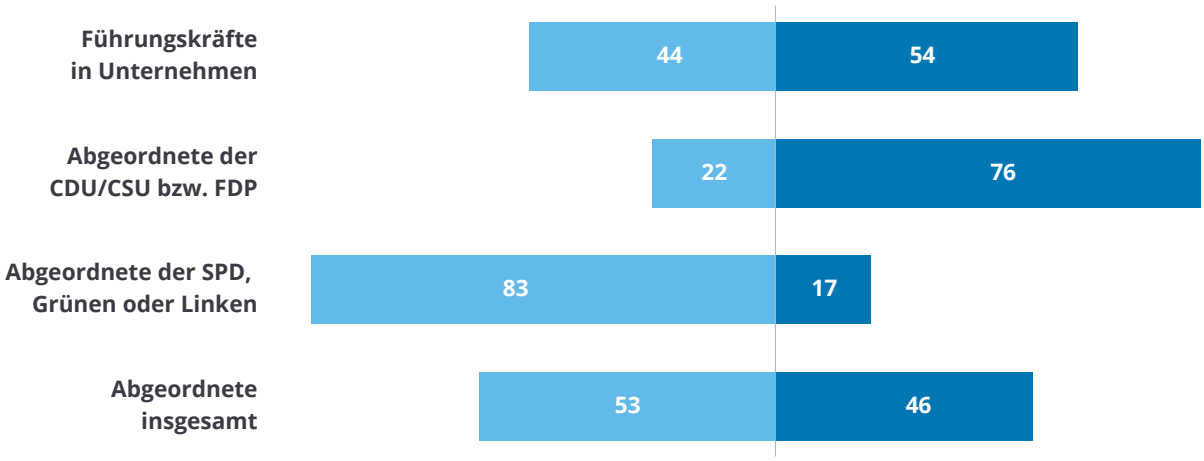
Aufgrund der vergleichsweisen großen Diffusion des Cyber-Raumes verschwimmen die Grenzen sowohl zwischen innerer und äußerer Sicherheit als auch zwischen „Cyber-Abwehr" und „Cyber-Verteidigung" zunehmend. In diese Gemengelage findet auch die Diskussion rund um die Frage statt, ob der deutsche Staat selbst Cyber-Angriffe durchführen soll und wie weit diese gehen sollen. So wird hier kontrovers die sogenannte „aktive Cyber-Verteidigung" diskutiert, welche – grob ausgedrückt – das Ausüben von Cyber-Angriffen aus Verteidigungszwecken meint. Daran angelehnt arbeitet auch die Bundesregierung gerade an der Schaffung eines rechtlichen Rahmens für sogenannte „Hack Backs", welche beispielsweise das Stilllegen von angreifenden Servern oder das Löschen von gestohlenen Daten umfassen.

Dass diese Thematik nicht unstrittig ist, zeigt sich auch bei der Befragung der Abgeordneten und Wirtschaftsführer: Eine knappe Mehrheit Letzterer votiert für die Schaffung solcher Offensivoptionen, eine knappe Mehrheit Ersterer ist dagegen. Bei den Politikern verläuft die Trennlinie dabei vor allem entlang der Parteizugehörigkeiten: Während sich rund drei Viertel der Abgeordneten von CDU, CSU und FDP dafür aussprechen, Möglichkeiten für eigene Cyber-Angriffe zu schaffen, nehmen 83 Prozent der Abgeordneten von SPD, Grünen und der Linken die Gegenposition ein. Die Abgeordneten der AfD votieren jeweils etwa zur Hälfte dafür bzw. dagegen. Diese parteipolitische Verteilung spiegelt auch die allgemeine Diskussion bezüglich dieser Thematik im Bundestag und in den Medien wider.

Abb. 16 – Soll Deutschland selbst in der Lage sein, Cyber-Angriffe durchzuführen?

Gespaltenes Meinungsbild bei Entscheidern aus Politik und Wirtschaft, ob Deutschland Cyber-Angriffe durchführen sollte.

- Finden es nicht richtig.
- Finden es grundsätzlich richtig, wenn Deutschland sich in die Lage versetzt, selbst Cyber-Angriffe durchzuführen zu können.



In Prozent der Nennungen

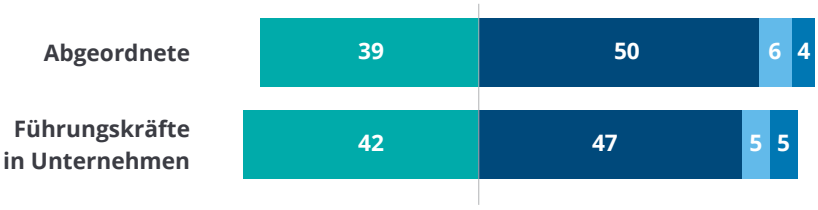
Einen Schritt weiter geht man bei der Frage, ob auch Unternehmen, wenn sie von Hackern angegriffen werden, das Recht haben sollten, selbst zurückzuschlagen. Von dieser Vorstellung sind jedoch weder Abgeordnete noch Wirtschaftsführer angetan. Jeweils lediglich 10 Prozent der beiden Befragtengruppen votieren dafür, wichtigen Unternehmen im Falle eines Cyber-Angriffs das Recht einzuräumen, selbst mit solchen Attacken gegen den Angreifer vorzugehen. Jeweils rund die Hälfte der Abgeordneten und Wirtschaftsführer vertritt den Standpunkt, dies sollte staatlichen Stellen vorbehalten bleiben.

Abb. 17 – Wer soll zurückschlagen dürfen?

Hack Back

Bei einem Hacker-Angriff auf ein Unternehmen in Deutschland sollte gegen den Angreifer vorgehen dürfen:

- Das betroffene Unternehmen
- Sowohl das betroffene Unternehmen als auch staatliche Stellen
- Staatliche Stellen
- Weder/noch

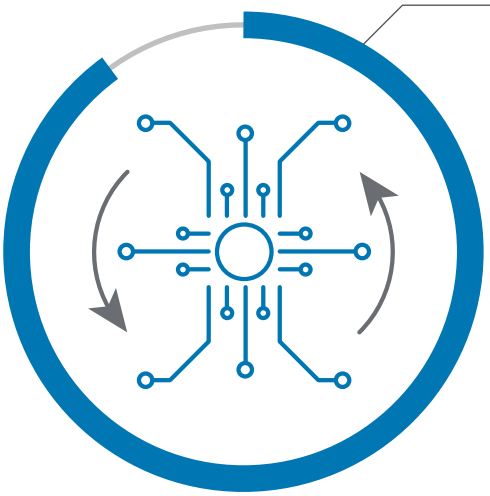


In Prozent der Nennungen

3.2 Hohe Erwartungen an staatliche Unterstützung

Digitalisierung und Cyber-Sicherheit sind zwei Seiten einer Medaille. Je mehr Wirtschafts- und Gesellschaftsbereiche von Digitalisierung und Vernetzung betroffen sind, desto mehr angreifbare Schnittstellen gibt es. Diese Durchdringung erfordert, Sicherheit von vornherein mitzudenken – „Security by Design". Erfolgreiche Digitalisierung schließt Cyber-Security mit ein, entscheidet so über zukünftige Entwicklungen in allen Lebensbereichen. Politische Entscheidungsträger haben dies auch erkannt. Digitalisierung spielt eine wichtige Rolle im Koalitionsvertrag, es gibt zahlreiche Initiativen in allen Ressorts, Bundesbehörden und auf Landesebene, aber reicht das und kommt es an?

Abb. 18 – Der Staat kann viel dazu beitragen, die Digitalisierung voranzubringen – das Getane wird aber als nicht ausreichend bewertet



90%

der **Entscheider** glauben, dass der Staat viel bis sehr viel zur Digitalisierung beitragen kann.

85%

der **Führungskräfte in Unternehmen** sind der Meinung, der Staat unterstützt den Prozess der Digitalisierung in Deutschland nicht ausreichend.

68%

der **Abgeordneten** sind der Meinung, der Staat unterstützt den Prozess der Digitalisierung in Deutschland nicht ausreichend.

Die Erwartungshaltung der Umfrageteilnehmer ist hoch.
Die Umfrageteilnehmer sind mit großer Mehrheit der Meinung, der Staat könne viel dazu beitragen, die Digitalisierung voranzutreiben. Sowohl Abgeordnete als auch Wirtschaftsführer sehen das zu rund 90 Prozent so. Mehr als ein Drittel sind darüber hinaus sogar überzeugt, der Staat könne sehr viel beitragen.

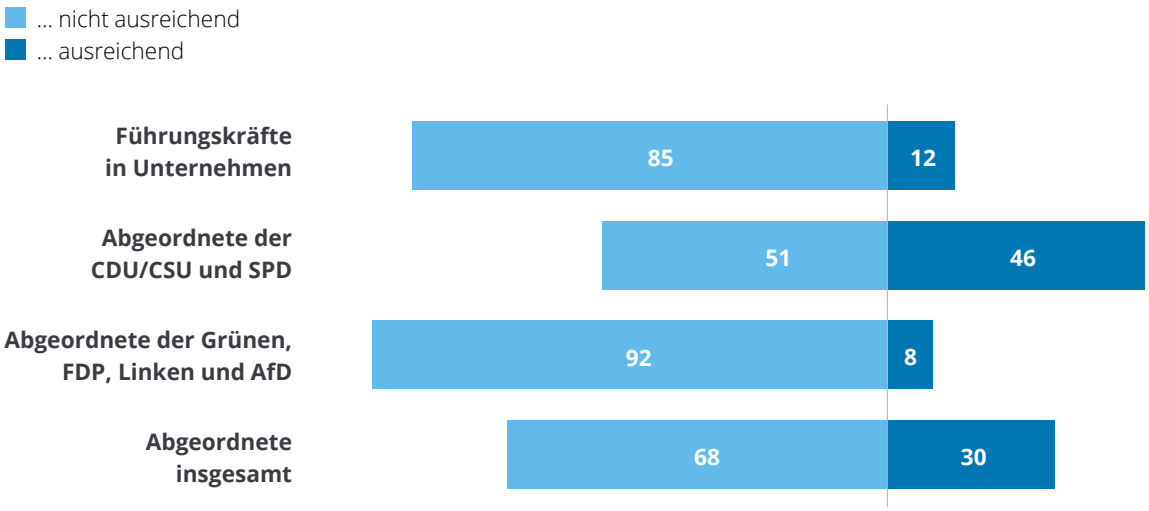
Doch zwischen den Aktivitäten der Politik und dem, was in der Praxis ankommt, scheint offenbar noch eine große Lücke zu klaffen. So ist die Mehrheit der Befragten der Meinung, dass der Staat bei der Digitalisierung hinter seinen Möglichkeiten bleibt. 85 Prozent der Führungskräfte halten die Unterstützung des Staates für die Digitalisierung für nicht ausreichend..

Es ist bereits viel auf den Weg gebracht, um Rahmenbedingungen für die Digitalisierung der Wirtschaft zu schaffen. Es gilt nun herauszufinden, welche Unterstützung der Wirtschaft konkret erforderlich ist, um die politischen Maßnahmen noch zielgerichteter darauf einzustellen."

Katrin Rohmann, Government & Public Services Industry Leader

Abb. 19 – Digitalisierung: Der Staat bleibt unter seinen Möglichkeiten

Top-Entscheider sind der Meinung, der Staat unterstützt den Prozess der Digitalisierung in Deutschland ...



In Prozent der Nennungen

Im Deutschen Bundestag widmet sich der Ausschuss Digitale Agenda netzpolitischen Themen und stellt entscheidende Weichen für den digitalen Wandel in Deutschland. Der Ausschuss selbst sieht sich als Impulsgeber für die parlamentarische Arbeit in dem Themenfeld.

Im Legislaturbericht vom April 2017 konstatiert die Bundesregierung, es seien die entscheidenden Schritte unternommen worden, um die Ziele der Digitalen Agenda zu erreichen, und dass Deutschland für die digitale Zukunft in vielen Bereichen gut vorbereitet sei.

Im aktuellen Koalitionsvertrag vom März 2018 sind der Digitalisierung 13 von 175 Seiten gewidmet und auch sonst ist das Wort „digital" ein zentraler Begriff im Vertrag.

Ziele des Koalitionsvertrages sind:

- Eine flächendeckende digitale Infrastruktur von Weltklasse
- Die Vermittlung von digitalen Fähigkeiten als Schlüsselkompetenz für alle Altersgruppen
- Eine Arbeitswelt, die Menschen für den digitalen Wandel befähigt und mehr Lebensqualität ermöglicht
- Eine Regulierung, die Wettbewerb und Wettbewerbsfähigkeit schafft
- Mehr Sicherheit im Cyber-Raum
- Mehr Bürgernähe durch eine moderne, digitale Verwaltung
- Ein Rechtsrahmen, der Bürgerrechte garantiert, einen Ausgleich von Freiheit und Sicherheit leistet und gleichzeitig mehr Innovationen ermöglicht

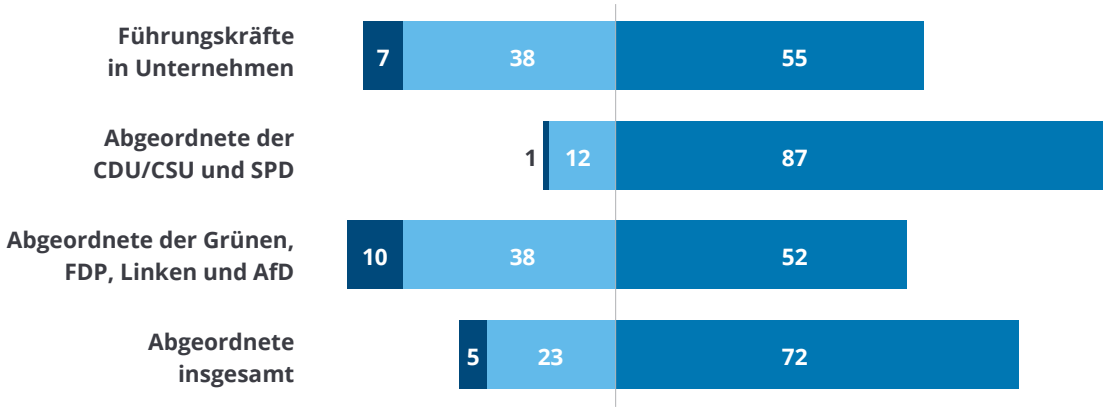
Mit der Staatsministerin für Digitalisierung im Bundeskanzleramt gibt es eine zentrale Stelle mit Verantwortung für die Digitalisierung. Seit August 2018 ist der Digitalrat eingesetzt, der die Bundesregierung bei der Digitalisierung und der digitalen Transformation beraten soll. Es gibt einen Kabinettsausschuss Digitalisierung, dem Kanzlerin, Finanzminister und Kanzleramtsminister vorsitzen, der Digitalisierung auf höchster Ebene abstimmen, Probleme diskutieren und Lösungen erarbeiten soll. Im November 2018 will das Kabinett eine gemeinsame Umsetzungsstrategie zur Steuerung der Digitalvorhaben beschließen.

Die Schwerpunktsetzung der Regierung wird anerkannt. Die Befragten bestätigen überwiegend, dass der Digitalisierung in dieser Legislaturperiode ein höherer Stellenwert beigemessen wird.

Abb. 20 – Höherer Stellenwert für Digitalisierung in dieser Legislaturperiode

Nach dem Eindruck der Top-Entscheider hat das Thema Digitalisierung für die Bundesregierung in dieser Legislaturperiode im Vergleich zur letzten …

- … einen niedrigeren Stellenwert
- … einen gleichwertigen Stellenwert
- … einen höheren Stellenwert



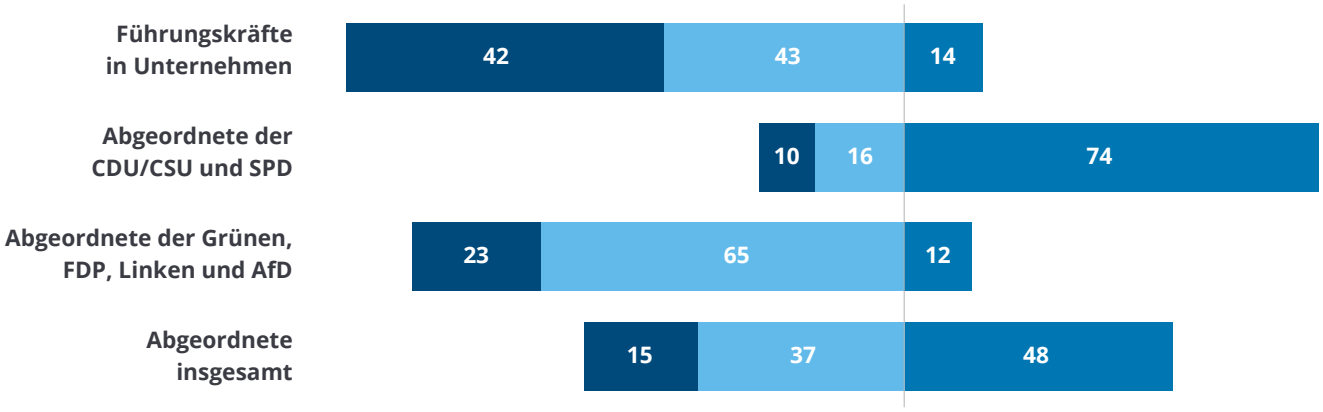
In Prozent der Nennungen

Während die Erwartungshaltung an den Staat hoch ist, sind die meisten Befragten davon überzeugt, dass der Staat mehr für die Digitalisierung des Wirtschaftsstandorts Deutschland machen könnte.

Abb. 21 – Falsche Schwerpunkte

Nach dem Eindruck der Top-Entscheider setzt die Bundesregierung bei der Digitalisierung ...

- ... nicht die richtigen Schwerpunkte
- ... die richtigen Schwerpunkte
- Können das nicht einschätzen



In Prozent der Nennungen

Bezüglich der politischen Schwerpunktsetzung gehen die Meinungen zwischen Wirtschaft und Politik auseinander. Insbesondere Politiker aus den Parteien der Regierungskoalition sehen das positiv: Rund drei Viertel haben den Eindruck, dass die Regierung im Bereich Digitalisierung die richtigen Schwerpunkte setzt. Die Wirtschaftsführer bewerten es dagegen eher so wie die Opposition, das heißt haben eher den gegenteiligen Eindruck. Zudem trauen sich viele Wirtschaftsführer erstaunlicherweise kein Urteil zu (42%), sie kennen offenbar die von der Politik gesetzten Schwerpunkte nicht ausreichend.

Die Digitalisierung ist zwar politisch auf der Agenda und es gibt eine sehr hohe Erwartungshaltung an den Staat. Diese wird derzeit jedoch auch deshalb nicht erfüllt, weil die Schwerpunkte häufig nicht als die richtigen bewertet werden oder nicht klar genug kommuniziert worden sind.

Somit gibt es an dieser Stelle Handlungsbedarf seitens der Politik – sowohl inhaltlich wie auch im Diskurs. Wenn ein Großteil aller Befragten der Meinung ist, dass der Staat unter seinen Möglichkeiten bleibt, muss man sich fragen, warum das so gesehen wird. Gleichzeitig gilt es auch herauszufinden, warum 42 Prozent der Führungskräfte nicht beurteilen können, ob der Staat die richtigen Schwerpunkte bei der Digitalisierung setzt.

Handlungsfelder

Evaluation der Digitalisierungspolitik der Bundesregierung
Damit der Wirtschaftsstandort Deutschland auch in der digitalisierten Welt eine Spitzenposition beibehält und weiter ausgebaut werden kann, bedarf es übergeordneter und koordinierter Strategien, die möglichst schnell und effektiv für die verschiedenen Handlungsfelder implementiert werden. Die Umsetzung der Ziele sollte fortlaufend evaluiert werden. Die Ziele müssen klar priorisiert und kommuniziert werden und messbar sein – besonders mit Blick auf den Nutzen für den Wirtschaftsstandort Deutschland und die Zukunftsthemen Big Data sowie künstliche Intelligenz.

Privat und Staat
Dem Staat wird eine starke Gestaltungsmacht bei der Digitalisierung zugesprochen, tatsächlich aber wird nur begrenzt wahrgenommen, wie und ob die Digitalisierung gefördert und vorangebracht wird. Deshalb sollte zur besseren Identifizierung, Planung und Umsetzung der Digitalisierungsprojekte ein intensiverer Stakeholder-Dialog geführt werden, um bisher nicht adressierte oder wahrgenommene Themen gemeinsam zu erörtern, die richtigen Schwerpunkte zu setzen und die erforderlichen Kompetenzen zu bündeln.

Vorbereitung auf Cyber-Angriffe auf Infrastruktur und staatliche Stellen als ungenügend wahrgenommen
Die Zweifel am Stand der Vorbereitung auf Cyber-Angriffe auf staatliche Stellen und Infrastruktur sind ernst zu nehmen und die getroffenen Maßnahmen auf ihre Wirksamkeit zu überprüfen. Über den Stand der Maßnahmen sind mehr Transparenz und Information erforderlich.

Zentralisierung, Standardisierung und Koordinierung von Informationen über Cyber-Bedrohungen
Die Unternehmen sind zunächst selbst in der Verantwortung für ihre Cyber- und Informationssicherheit. Für übergreifende Sicherheitsfragen brauchen sie jedoch staatliche Unterstützung und Austausch. Gewünscht wird vor allem eine Information über aktuelle Gefährdungen, ein zeitnahes Warnsystem vor Attacken und Unterstützung im Falle eines Angriffs.

Debatte über aktive Cyber-Verteidigung erforderlich
Es finden sich viele Befürworter dafür, dass Deutschland auch die Fähigkeit besitzen soll, aktiv Cyber-Angriffe durchführen zu können. Die Durchführung eines digitalen Gegenangriffs sollte in staatlicher Verantwortung sein. Dazu müsste auf staatlicher Ebene geregelt werden, wie die Verfahren zu einer eindeutigen Attribution sind, wie aktive Cyber-Verteidigung zu verstehen ist und wer wann und wie handeln darf.

Ansprechpartner

Katrin Rohmann
Government & Public Services Industry Leader
Tel: +49 (0)30 25468 127
krohmann@deloitte.de

Peter J. Wirnsperger
Cyber Risk Leader
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Deloitte.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden, und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk") erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL"), eine „private company limited by guarantee" (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global" genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Risk Advisory, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für rund 286.000 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.

Stand 10/2018