Deloitte.

Cyber Security Report 2019

Teil 1: Fake News und Schlüsseltechnologien – wachsende Herausforderungen

Vorwort

Die digitale Transformation verändert unaufhaltsam die Art und Weise, wie wir arbeiten und leben. Innovationen und Schlüsseltechnologien sind die Treiber dieser Veränderung. Ein nachhaltiger Erfolg dieser Treiber benötigt angemessene regulatorische Rahmenbedingungen und Führungskräfte, die ihre Unternehmen darauf einstellen.

Mit der digitalen Transformation einher geht auch eine schwer zu antizipierende Bedrohungs- und Gefährdungslage, die durch adäquate Cyber-Security-Maßnahmen adressiert werden muss. Nur so können Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Prozessen gewährleistet werden und Innovationen sowie Schlüsseltechnologien zum nachhaltigen und sicheren Erfolg genutzt werden.

Im Rahmen unserer Cyber-Security-Projekte beobachten wir diese Herausforderungen seit vielen Jahren und begleiten unsere Kunden bei der Umsetzung von Lösungen.

Gemeinsam mit dem Institut für Demoskopie Allensbach hat Deloitte im neunten Jahr in Folge eine repräsentative Trendstudie durchgeführt, um den Stand der Cyber Security in Deutschland zu erheben. Befragt wurden 408 Führungskräfte aus Unternehmen sowie 115 Abgeordnete aus Länderparlamenten, Deutschem Bundestag und Europaparlament zu Cyber-Risiken und den daraus folgenden Gefahren für Staat und Unternehmen.

Politiker und Wirtschaftsführer geben ihre Einschätzung zur Bedrohung durch Cyber- und IT-Risiken, berichten über die Zahl der erfolgten Angriffe, die Art der daraus folgenden Schäden und die von ihnen ergriffenen Maßnahmen in den Unternehmen und beim Setzen der Rahmenbedingungen in Deutschland. Die Ergebnisse zeigen auf, wie Entscheider die aktuelle Gefährdung einschätzen, welche Maßnahmen sie bereits umgesetzt haben und wo künftige Handlungsfelder für Staat und Wirtschaft liegen.

Wir haben den Fokus der Trendstudie in diesem Jahr um wesentliche Punkte der aktuellen Situation in den Unternehmen und wichtige Fragestellungen aus der gesellschaftlichen und politischen Debatte ergänzt:

- Nationale Rahmenbedingungen für die IT-Sicherheit
- Manipulation der Meinungsbildung und Fake News
- Schlüsseltechnologien für die Digitalisierung
- Fachkräfte für IT-Sicherheit

Wir haben im hier vorliegenden Teil 1 der Studie auf die gesamtgesellschaftliche und politische Ebene sowie das Zusammenspiel von Staat und Wirtschaft abgestellt. Teil 2 wird über die Gefährdungen und Gegenmaßnahmen in Unternehmen berichten.

Vorwort 02

Executive Summary 04

1. Einschätzung der Gefährdung 06

2. Meinungsmanipulation durch Fake News 10

    2.1 Begriffsbestimmung 10

    2.2 Fake News – Staatsfeind Nr. 1? 12

3. Schlüsseltechnologien für Cyber-Sicherheit 16

4. Verantwortung von Staat und Wirtschaft 18

5. Rahmenbedingungen für Standort 21

Handlungsfelder 28

Ansprechpartner 30

Executive Summary

Viele Cyber-Risiken werden von jeweils deutlichen Mehrheiten der Entscheidungsträger in Wirtschaft und Politik als großes Risiko für die Menschen in Deutschland eingestuft. Tendenziell werden die Cyber-Risiken für die Menschen in Deutschland von den Wirtschaftsführern höher eingeschätzt als von Abgeordneten.

Meinungsmanipulation und Fake News sind höchstes Risiko
Unter den Cyber-Gefahren belegt die Manipulation der öffentlichen Meinung z.B. durch Fake News dabei erstmals den Spitzenplatz des Rankings. Politiker sehen im steigenden Einfluss der sozialen Medien daneben zur Hälfte eine Gefahr für die Demokratie; für die jeweils eigene Partei jedoch mehrheitlich Chancen.

Gute Rahmenbedingungen für die IT-Sicherheit in Deutschland
Die rechtlichen Rahmenbedingungen für IT-Sicherheit werden für Deutschland, verglichen mit anderen Ländern, von einer Mehrheit der Entscheidungsträger gut eingeschätzt. Insbesondere Vertreter größerer Unternehmen urteilen hier sehr positiv. Die Rahmenbedingungen beeinflussen Standortentscheidungen jedoch kaum. Lediglich bei der Auswahl von IT-Dienstleistern, wie bspw. für Cloud-Services, ist der Standort sehr relevant.

Fehlende Unabhängigkeit bei Schlüsseltechnologien – Gefahr für die Cyber-Sicherheit?
Eine europäische Unabhängigkeit bei der Entwicklung von Schlüsseltechnologien gilt für die überwiegende Mehrheit der Abgeordneten und Wirtschaftsführer als notwendig für die Cyber-Sicherheit in Deutschland. Allerdings werden zum Einsatz von Technologien aus den USA oder China, z.B. beim Ausbau des 5G-Netzes, derzeit keine Alternativen gesehen. Diese Abhängigkeit wird von vielen Befragten als große Gefahr bewertet.

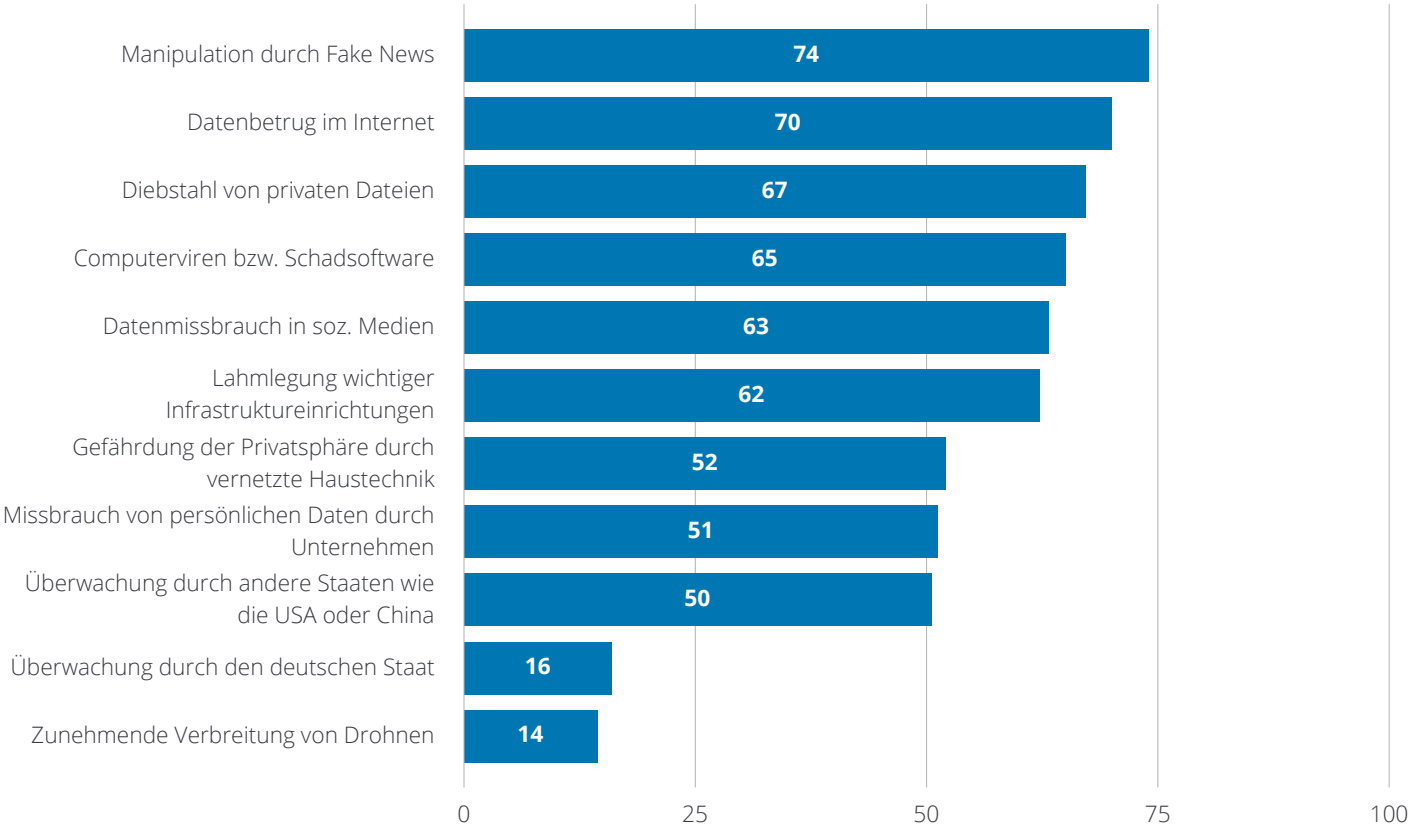
Staat und Wirtschaft
Die Politik kann zur Erhöhung der IT-Sicherheit in Unternehmen beitragen, davon sind Politiker und Wirtschaftsvertreter überzeugt. Allerdings sehen derzeit fast drei Viertel von Letzteren die Bedürfnisse der Wirtschaft in diesem Bereich nicht gut durch staatliche Institutionen abgedeckt. Die Hälfte der Abgeordneten hingegen fühlt sich nicht gut über Probleme und Bedürfnisse der Wirtschaft beim Thema IT-Sicherheit informiert. Beide Seiten beklagen daher einen mangelnden Austausch zwischen Politik und Wirtschaft.

NEWS

1. Einschätzung der Gefährdung

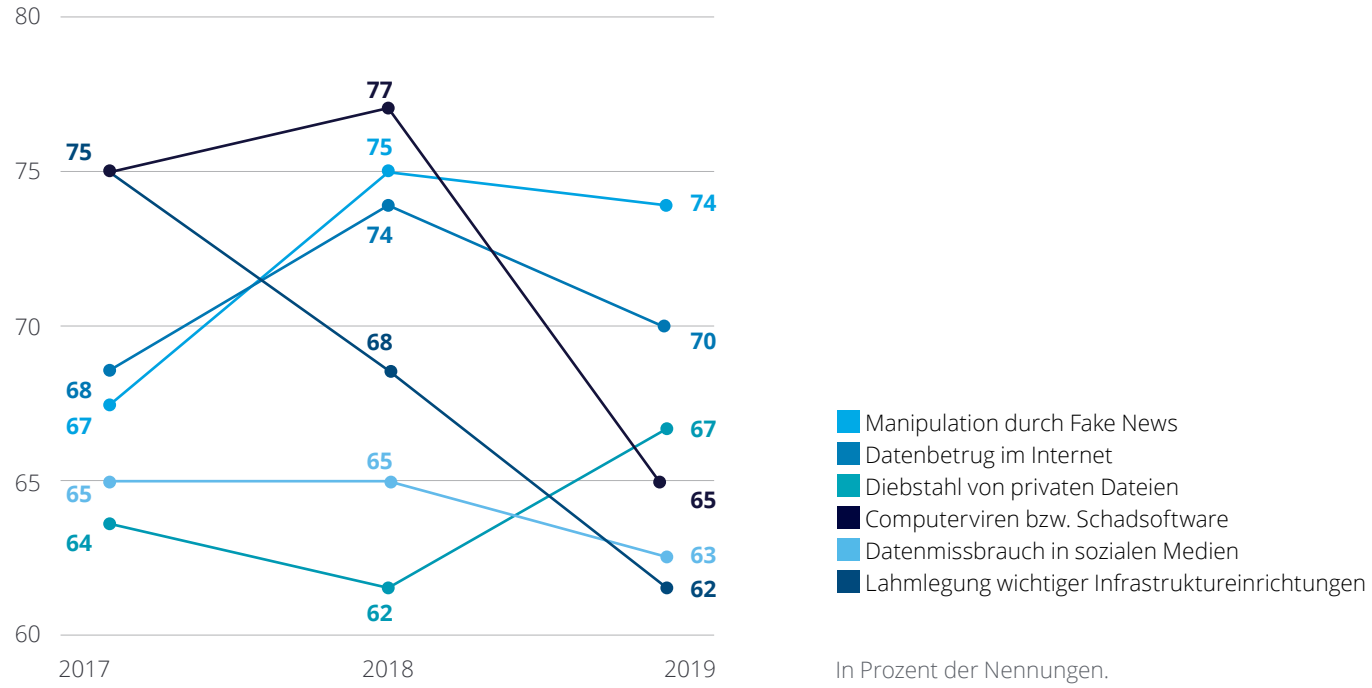
In Fake News – der Manipulation der öffentlichen Meinung durch gefälschte oder irreführende Nachrichten – sehen in diesem Jahr für 74 Prozent der Entscheidungsträger ein großes Risiko für die Menschen in Deutschland. In den vergangenen Jahren waren es 67 Prozent (2017) bzw. bereits 75 Prozent (2018). 2019 wurde kein anderes der insgesamt elf abgefragten Risiken so häufig als groß eingestuft. In der Rangliste der als hoch eingestuften Gefahren folgen Datenbetrug im Internet (von 70 Prozent der Befragten genannt), Diebstahl von privaten Dateien und Informationen durch Cyber-Angriffe (67 Prozent), Computerviren bzw. Schadsoftware (65 Prozent), der Missbrauch von persönlichen Daten durch andere Nutzer in sozialen Netzwerken (63 Prozent) und das Lahmlegen von wichtigen Infrastruktureinrichtungen (62 Prozent). Auch in den vergangenen zwei Jahren wurden diese Risiken als die sechs bedeutendsten Gefahren wahrgenommen.

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



In Prozent der Nennungen.

Abb. 2 – Top 6 der größten Cyber-Risiken in Deutschland (2017–2019)

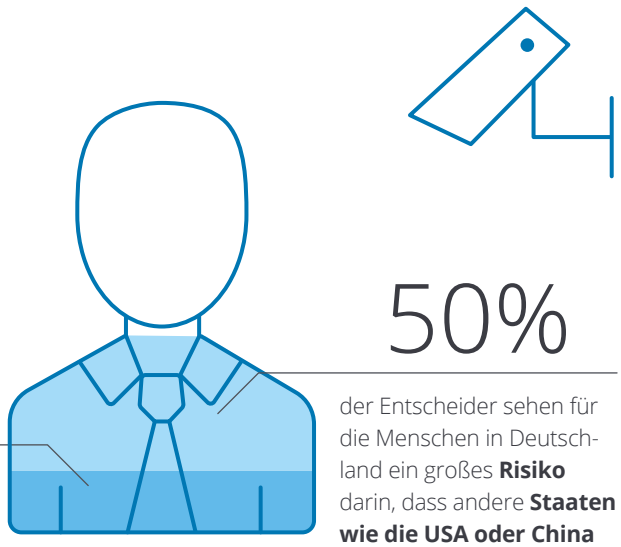


Die Gefahr durch Computerviren und Schadsoftware erhielt im vergangenen Jahr noch die meisten Nennungen als hohes Risiko (77 Prozent). In diesem Jahr sagten das lediglich 65 Prozent der Befragten: Platz vier. Angriffe auf Stromnetze oder Krankenhäuser wurden 2017 noch am häufigsten als hohes Risiko eingestuft (75 Prozent). In diesem Jahr teilten nur noch 62 Prozent diese Einschätzung. Die Gefahr eines Ausfalls von kritischen Infrastruktureinrichtungen rutscht 2019 damit auf Platz sechs der Risikorangliste ab. In den beiden Vorjahren noch auf Platz sechs, rangiert Diebstahl von privaten Dateien und Informationen jetzt auf dem dritten Platz der als hoch bewerteten Risiken.

Rund die Hälfte der Befragten sah in diesem Jahr jeweils ein hohes Risiko in der Gefährdung der Privatsphäre durch die zunehmende Vernetzung von Haushaltsgeräten, den Missbrauch von persönlichen Daten durch Unternehmen und die Überwachung deutscher Bürger durch andere Staaten.

Eine Überwachung durch den eigenen Staat sehen hingegen nur 16 Prozent der Befragten als hohes Risiko. Gefährdungen im Zusammenhang mit der staatlichen Überwachung von Bürgern sehen die Entscheider viel stärker als „Spionagethema“, das heißt als Risiko der Überwachung durch fremde Staaten, wie die USA oder China. Daran hat sich in den vergangenen fünf Jahren auch nichts grundlegend geändert.

Abb. 3 – Überwachung durch staatliche Akteure



16%

der Entscheider sehen für die Menschen in Deutschland ein großes **Risiko** darin, dass der **deutsche Staat die Bürger zu sehr überwacht.**

50%

der Entscheider sehen für die Menschen in Deutschland ein großes **Risiko** darin, dass andere **Staaten wie die USA oder China die deutschen Bürger überwachen.**

Während es bei den Top-6-Risiken teilweise große Änderungen gab, sind die folgenden fünf Risiken in Bezug auf Rangplatz und Anzahl der Nennungen in den vergangenen Jahren verhältnismäßig unverändert geblieben.

Die befragten Abgeordneten bewerten – im Vergleich zu den Wirtschaftsführern – die meisten der genannten Gefahren seltener als hohes Risiko. Die größten Unterschiede in der Einstufung gab es bei den Gefahren durch Datenbetrug im Internet. 73 Prozent der Wirtschaftsführer nannten dies als hohes Risiko für die Menschen in Deutschland von den Abgeordneten lediglich 58 Prozent. Ebenfalls große Abweichungen gab es bezüglich der Risikoeinschätzung zum Diebstahl von privaten Dateien und Informationen, zu Schadsoftware und Computerviren sowie zum Schutz der Privatsphäre durch die zunehmende Vernetzung von Hausgeräten.

„Die Entscheider in der Wirtschaft haben großes Vertrauen in unsere Regierungsorganisationen, wenn nur 16 Prozent in der Überwachung durch den deutschen Staat ein Risiko sehen. Dieses sollte als Basis für einen intensiven Austausch genutzt werden."

Katrin Rohmann, Government & Public Services Industry Leader

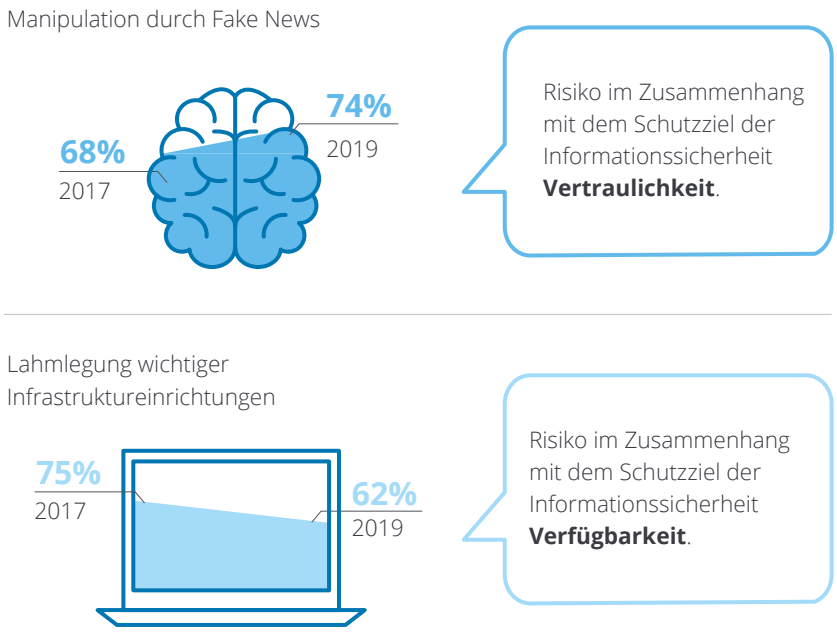
Computerviren können die private oder geschäftliche Nutzung von Software oder Computersystemen gefährden. Dies kann zu Einschränkungen im Privatleben des einzelnen Bürgers oder der Geschäftstätigkeit von Unternehmen führen. Sogar als selbstverständlich angenommene gesellschaftliche Funktionen – beispielsweise die Erzeugung und Verteilung von elektrischem Strom oder die Notfallversorgung in Krankenhäusern – könnten durch einen koordinierten Einsatz von Schadsoftware geschädigt werden. Die im Kontext Verfügbarkeit von Informationstechnik genannten Risiken werden seltener als hoch eingeschätzt.

Integrität und Vertraulichkeit gelten – neben Verfügbarkeit – als Schutzziele der Informationssicherheit. Die Verbreitung von Fake News, der Diebstahl von privaten Daten, aber auch der Missbrauch von persönlichen Daten in sozialen Netzwerken oder Datenbetrug im Internet sind Risiken für diese beiden Schutzziele.

Seit 2017 stieg bei den Befragten die Einstufung des Risikos, dass die öffentliche Meinung durch Fake News manipuliert wird, am stärksten an. Dagegen ging die Wahrnehmung, dass wichtige Infrastruktureinrichtungen wie Stromnetze oder Krankenhäuser durch einen Cyber-Angriff lahmgelegt werden, am stärksten zurück.

Mit anderen Worten: die Bewertung einer Gefährdung von Vertraulichkeit von Informationen stieg am stärksten an und die Bewertung einer Gefährdung der Verfügbarkeit von Informationstechnik ging am stärksten zurück.

Abb. 4 – Größtes Cyber-Risiko in Deutschland 2017 und 2019 im Vergleich



2. Meinungsmanipulation durch Fake News

Einer der größten gesellschaftlichen Umbrüche des letzten Jahrzehnts ist der Siegeszug der sozialen Medien. Sie vernetzen Nutzer aus aller Welt und eröffnen neue Kommunikationswege für Unternehmen. Inzwischen ist aber auch die Kehrseite dieser Medaille unübersehbar. Soziale Medien können ebenso als Instrument der Manipulation der öffentlichen Meinung dienen, etwa durch gezielte Falschmeldungen oder verzerrte Darstellung von Sachverhalten. Durch zielgruppenorientierte Platzierung verbreiten sich diese dann viel schneller als in etablierten Medien, ohne dass ein eindeutiger Urheber oder Verleger presserechtliche Verantwortung übernehmen würde. Hinter den Meldungen stehende Interessengruppen sind häufig nicht erkennbar. Das Thema „Fake News" beherrscht heute die Schlagzeilen und ist so drängend, dass es 2019 erstmals den Sprung auf den unrühmlichen „Platz eins" der Liste der bedeutendsten Cyber-Risiken geschafft hat – sicherlich eines der aufsehenerregendsten Ergebnisse der Studie.

Begriffsbestimmung

Desinformationen zielen darauf ab, eine Einflussnahme auf die Zielgruppe zu erzeugen und damit politische Stimmungsbilder zu manipulieren oder wirtschaftliche Gewinne zu erzielen. Desinformationen werden heutzutage häufig in Textform produziert und mit gefälschten oder aus dem Kontext gerissenen Bildern unterlegt. Durch technologische Entwicklung wurden in letzter Zeit auch vermehrt „Deepfakes" erstellt. Dabei handelt es sich um gefälschte Videos, bei denen die Identifizierung der Fälschung zunehmend schwieriger durchzuführen ist. Die Verbreitung von Desinformation findet durch technologische Unterstützung (z.B. Algorithmen und Bots) meist über soziale Medien, Internetforen und Nachrichten-/Messenger-Dienste statt. Zusätzlich spielt auch die Verbreitung durch Nutzer, die Desinformationen nicht erkennen, eine erhebliche Rolle.

Die erfolgreiche Verbreitung von Desinformation kann enorme Auswirkungen auf die Gesellschaft haben und eine Bedrohung für demokratische politische Prozesse und Entscheidungsfindungen sein. Zusätzlich kann sie zu wirtschaftlichen Schäden führen, einen Einfluss auf öffentliche Güter und die Umwelt haben und die Gesundheit und Sicherheit von Bürgern gefährden.[1] Im Folgenden sind einige bekannte Beispiele von identifizierten Fake News aufgezeigt.

[1] Europäische Kommission (2018)

Abb. 5 – Beispiele für identifizierte Fake News

Um die von Desinformation ausgehende Gefahrenlage einschätzen zu können und um Gegenmaßnahmen zu ergreifen, ist eine Abgrenzung des Begriffs unabdingbar. Umgangssprachlich wird zumeist „Fake News" verwendet. Der Begriff ist allerdings problematisch. Zum einen schließt er andere Formen von fehlerhafter Kommunikation mit ein, wie beispielsweise ungewollte Fehler in journalistischer Berichterstattung. Zum anderen wird der Begriff auch von politischen Akteuren und deren Anhängern instrumentalisiert, indem abweichende politische Meinungen als Fake News degradiert werden. Aus diesem Grund wird in fachlichen Kreisen hauptsächlich der Begriff „Desinformation" favorisiert.[2]

Die EU-Kommission definiert Desinformation als „(...) nachweislich falsche oder irreführende Informationen, die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können"[3]. Weiterhin legt die EU-Kommission fest, dass konzeptionell und begrifflich Desinformation klar von Informationen abgegrenzt werden muss, die zwar nicht unbedingt faktisch fundiert sind, allerdings im Rahmen des Rechts auf Meinungsfreiheit trotzdem eine Daseinsberechtigung haben. Das beinhaltet zum Beispiel Satire, Parodien oder klar gekennzeichnete parteiliche Nachrichten.[4]

Die Bundesregierung definiert Desinformation, ähnlich wie die EU-Kommission, „(...) als bewusst unrichtige Nachrichten und gezielte Falschmeldungen (...), die vortäuschen, vertrauenswürdige journalistische Angebote oder verlässliche Informationsgrundlagen zu sein"[5]. Sie betrachtet zudem Desinformationen als Teil von hybriden Risiken, also Bedrohungen, die sowohl aus militärischen als auch nichtmilitärischen Mitteln bestehen.[6] Dabei stellt die Steuerung von Diskussionen in sozialen Medien als auch die gezielte Manipulation von Information ein nicht-militärisches Konfliktmittel dar. Um diesen hybriden Bedrohungen besser zu begegnen, setzt die Bundesregierung zunehmend auf den Gedanken der „vernetzten Sicherheit", wobei die Kooperation zwischen Staaten und mit der EU zunehmend wichtiger wird.[7]

Um Desinformation anzugehen, hat die EU-Kommission eine Reihe an Maßnahmen ergriffen. Auf institutioneller Ebene wurde ein Rapid-Alert-System etabliert und die East StratCom Task Force der EEAS nahm ihre Arbeit auf. Zudem wurden einige strategische Dokumente wie beispielsweise der Aktionsplan gegen Desinformation publiziert. Ziel dieser Maßnahmen ist es, Desinformationen effizienter aufzuspüren, Kooperation innerhalb der EU zu stärken, den privaten Sektor mit einzubeziehen und das Bewusstsein der Bevölkerung zu fördern.

[2] High-level Group on fake news and online disinformation
[3] Europäische Kommission (2018)
[4] EU Codex zum Thema Desinformation
[5] Bundesregierung (2018)
[6] Bundestagsdrucksache 18/8904
[7] BMVg (2019)

Fake News – Staatsfeind Nr. 1?

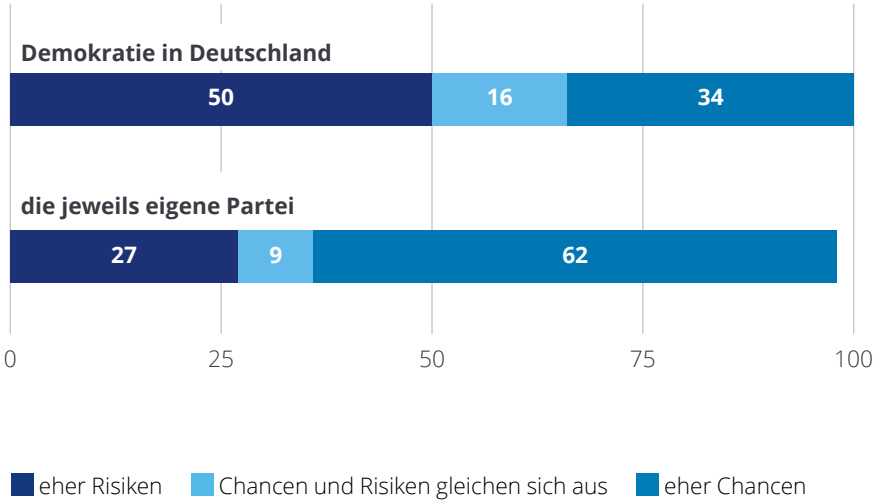
Die Manipulation der öffentlichen Meinung durch Fake News wird erstmals als größte Cyber-Gefahr für die Menschen in Deutschland bewertet: 74 Prozent der Entscheidungsträger aus Politik und Wirtschaft sehen in Fake News eine große Gefahr. Abgeordnete sehen aber nicht nur große konkrete Risiken durch die Manipulation der öffentlichen Meinung, sondern halten den zunehmenden Einfluss sozialer Medien auf die politische Meinungsbildung auch grundsätzlich eher für eine Gefahr für die Demokratie in Deutschland. Für die jeweils eigene Partei sehen Politiker in sozialen Medien dagegen ganz überwiegend eher Chancen als Risiken.

Besonders kritisch stehen Vertreter der CDU, CSU und SPD den sozialen Medien gegenüber. Rund zwei Drittel sehen in ihnen eher Risiken für die Demokratie, nur knapp ein Viertel eher Chancen, für die eigene Partei in ähnlich großen Anteilen Risiken wie Chancen.

Sowohl die Abgeordneten als auch die Parteien verfolgen in der Regel, was in den sozialen Medien über die jeweilige Partei geäußert wird.

Abb. 6 – Einfluss sozialer Medien

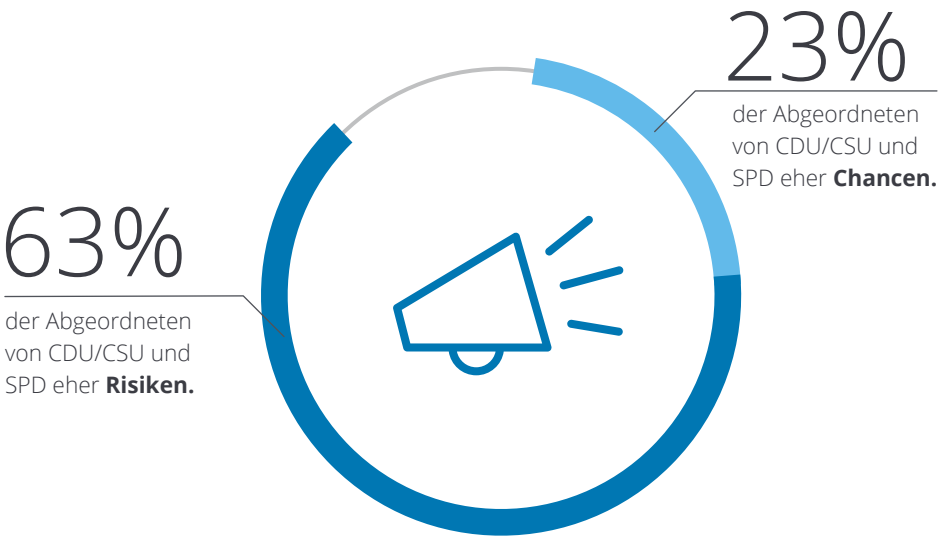
Im steigenden Einfluss sozialer Medien auf die politische Meinungsbildung sehen die Abgeordneten für die …



In Prozent der Nennungen. Auf 100 fehlende Prozent: unentschieden

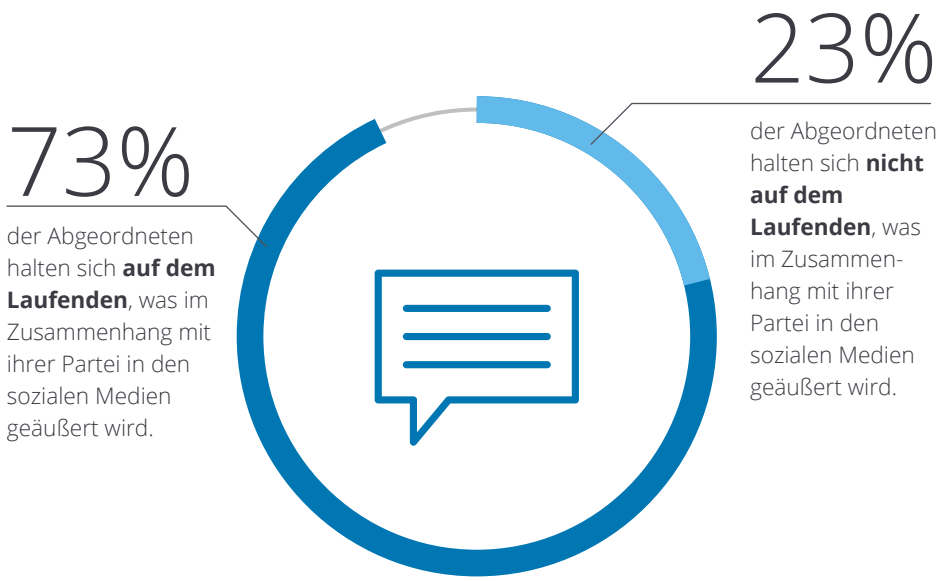
Abb. 7 – Chancen und Risiken sozialer Medien

Im steigenden Einfluss sozialer Medien auf die politische Meinungsbildung sehen für die Demokratie in Deutschland ...



Auf 100 fehlende Prozent: unentschieden.

Abb. 8 – Soziale Medien im Blick der Politiker
Parteien und Politiker verfolgen in der Regel das Echo in sozialen Medien.



Auf 100 fehlende Prozent: unentschieden.

Auch Unternehmen erwachsen aus den sozialen Netzwerken Bedrohungen. Ein Viertel der Befragten berichtet davon, dass es schon Versuche gegeben hat, den Ruf des Unternehmens durch gezielte Falschinformationen im Internet zu schädigen.

Fast jede zweite Top-Führungskraft aus mittleren und großen Unternehmen hält Falschinformationen im Netz auch für ein großes wirtschaftliches Risiko für das eigene Unternehmen, überdurchschnittlich häufig Führungskräfte von Unternehmen aus dem Dienstleistungssektor.

Nur rund die Hälfte der Studienteilnehmer verfolgt systematisch, was in sozialen Netzwerken über ihr Unternehmen geäußert wird, darunter überdurchschnittlich häufig größere Unternehmen, unterdurchschnittlich häufig dagegen bemerkenswerterweise Unternehmen, deren Führungskräfte in sozialen Netzwerken eher Risiken als Chancen für ihr Unternehmen sehen.

Insgesamt nehmen Wirtschaftsführer soziale Netzwerke aber deutlich eher als Chance für ihr Unternehmen denn als Risiko wahr.

Abb. 9 – Rufschädigung durch Falschinformation

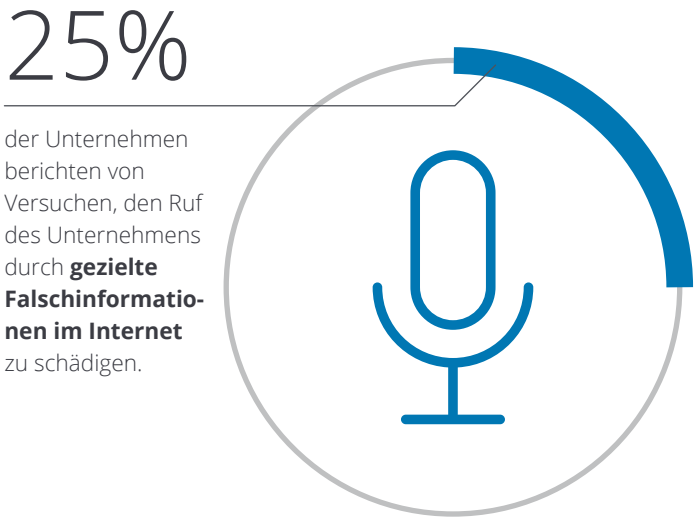
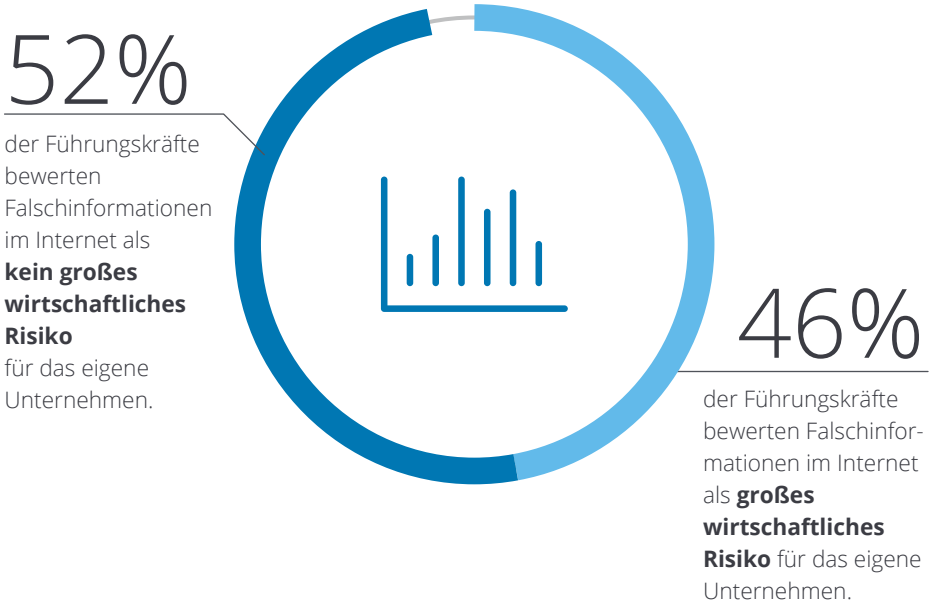


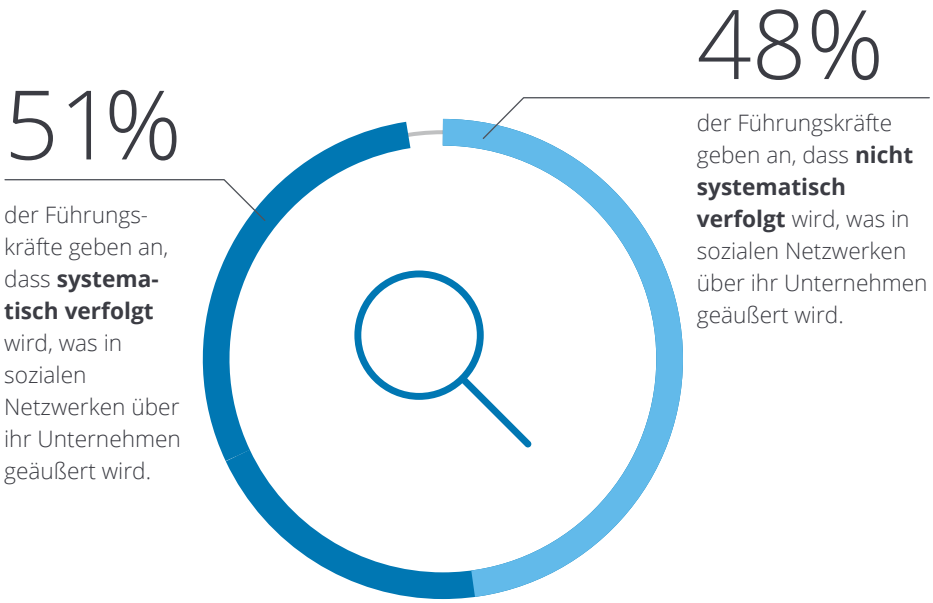
Abb. 10 – Wirtschaftliches Risiko aus Falschinformationen



Auf 100 fehlende Prozent: unentschieden.

Abb. 11 – Soziale Medien im Blick der Wirtschaft

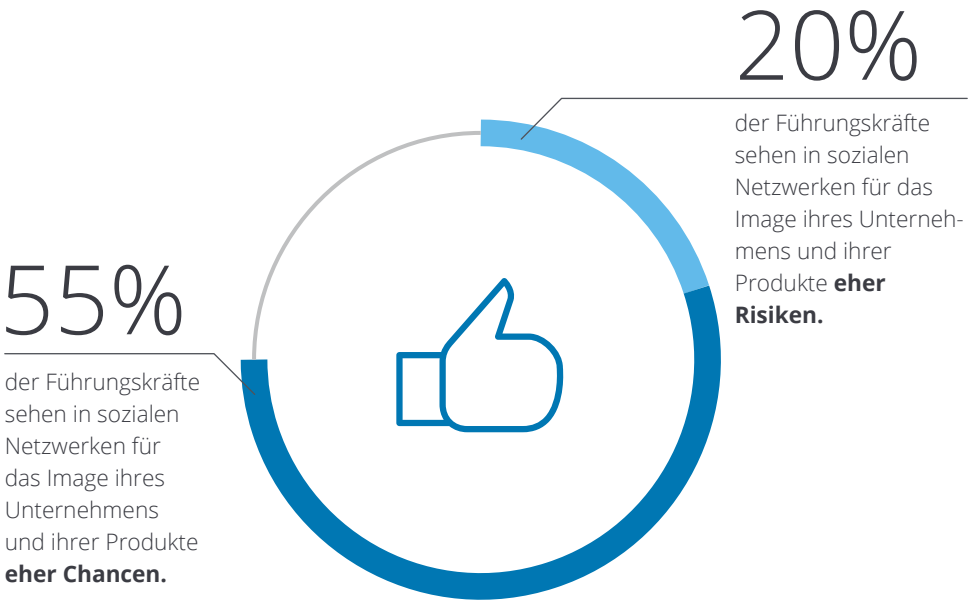
Viele Unternehmen verfolgen das Echo in sozialen Medien nicht systematisch.



Auf 100 fehlende Prozent: unentschieden.

Abb. 12 – Chancen und Risiken für Unternehmen durch soziale Netzwerke

Soziale Netzwerke stellen für Unternehmen eher Chancen als Risiken dar.



Auf 100 fehlende Prozent: unentschieden.

3. Schlüsseltechnologien für Cyber-Sicherheit

Schlüsseltechnologien sind Treiber der Zukunft. Sie zielen auf die Entwicklung von neuen Technologien und Innovationen. Aufgrund ihrer volkswirtschaftlichen Hebelwirkung sind sie von besonderer Bedeutung für die Zukunftsfähigkeit einer Gesellschaft.

Die Bundesregierung sieht unter anderen in der Informations- und Kommunikationstechnologie, der Mikroelektronik, der Quantentechnologie sowie in der Mensch-Technik-Interaktion besonderes Innovationspotenzial für neuartige und originelle Produkte, Verfahren und Dienstleistungen. Schlüsseltechnologien und Innovationen in den Bereichen können die starke Position und weltweite Wettbewerbsfähigkeit der deutschen Industrie sichern.[8]

89 Prozent der Abgeordneten und 71 Prozent der Wirtschaftsführer sind der Auffassung, dass wichtige Schlüsseltechnologien für die Digitalisierung und Vernetzung von deutschen oder europäischen Unternehmen hergestellt werden sollten und man sich unabhängig von anderen Ländern machen sollte, um ausreichende Cyber-Sicherheit in Deutschland zu gewährleisten.

Allerdings sehen beim Aufbau des 5G-Netzes nur 7 Prozent der Abgeordneten und 6 Prozent der Wirtschaftsführer derzeit ernsthafte Alternativen zu Technologien aus den USA oder China. Immerhin sind die Abgeordneten mehrheitlich davon überzeugt, dass es solche Alternativen in einigen Jahren geben könnte.

Wirtschaftsführer teilen dagegen eher die Überzeugung, dass wir auch langfristig keine Alternativen zu Technologien aus den USA oder China haben werden.

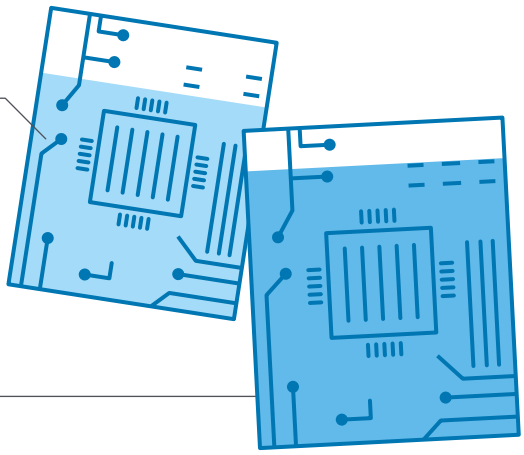
Von den Entscheidern, die derzeit keine technologischen Alternativen sehen, hält die Hälfte diese Abhängigkeit für eine große Gefahr. Insgesamt sehen das 40 Prozent der Top-Entscheider so.

Abb. 13– Schlüsseltechnologien made in EU

Um eine ausreichende Cyber-Sicherheit in Deutschland zu gewährleisten, müssen wichtige Schlüsseltechnologien für die Digitalisierung und Vernetzung von deutschen oder europäischen Unternehmen hergestellt werden.

71%

der Wirtschaftsführer sehen das so.



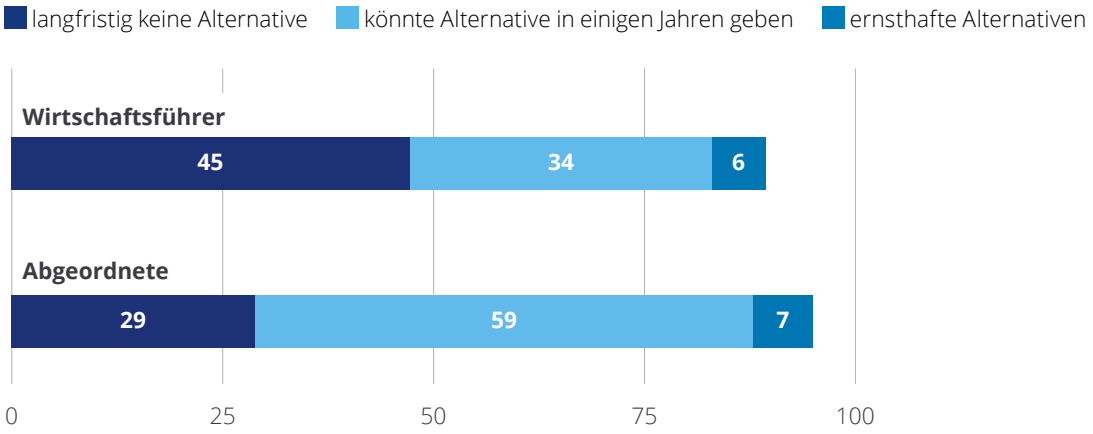
89%

der Abgeordneten sehen das so.

[8] Bundesbericht Forschung und Innovation (2018)

Abb. 14 – Aufbau des 5G-Netzes

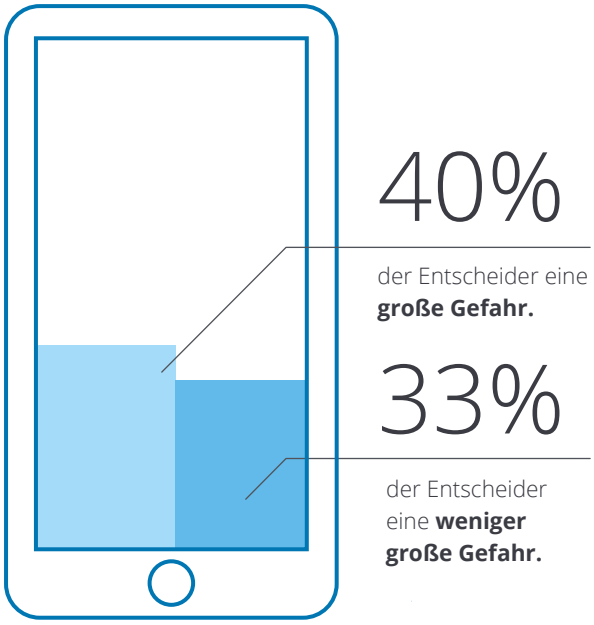
Beim Aufbau des 5G-Netzes hat Deutschland zu Technologien aus den USA und China ...



In Prozent der Nennungen.
Auf 100 fehlende Prozent: unentschieden

Abb. 15 – Abhängigkeit Deutschlands von 5G-Technologien

In der Abhängigkeit Deutschlands beim Aufbau des 5G-Netzes von Technologien Chinas und der USA sehen ...



Auf 100 fehlende Prozent: unentschieden bzw. "gar keine Gefahr".

„Die Verbreitung von neuen Informations- und Kommunikationstechnologien erfolgt immer schneller, Maßnahmen zum Schutz und für die Informationssicherheit sollten im Gleichschritt entwickelt werden. Insbesondere bei neuen Schlüsseltechnologien und Sprunginnovationen ist das Voraussetzung für eine erfolgreiche und sichere Digitalisierung."

Peter Wirnsperger, Cyber Risk Leader

4. Verantwortung von Staat und Wirtschaft

Bedrohungsszenarien und Herausforderungen – davon gibt es viele im Bereich Cyber Risk. Aber es gibt auch positive und optimistisch stimmende Aussagen. Wirtschaftsführer und Abgeordnete teilen die Auffassung, dass die Politik zur Bekämpfung von Cyber-Risiken in Unternehmen beitragen kann. Voraussetzung dafür ist stärkerer Informationsaustausch, denn bisher kennen sich nur 9 Prozent der Top-Manager mit staatlichen Einrichtungen im Bereich der Cyber-Sicherheit relativ gut aus, und nur rund die Hälfte der Abgeordneten fühlt sich gut oder sehr gut über die Bedürfnisse der Wirtschaft auf dem Gebiet informiert. Über 80 Prozent sowohl der Unternehmensvertreter als auch der Abgeordneten plädieren daher für einen verstärkten Austausch.

Breite Akzeptanz

Ein positiver Aspekt ist die breite Akzeptanz der Möglichkeiten von Staat und Politik, zur Bekämpfung von Cyber-Risiken beizutragen: 89 Prozent der Wirtschaftsvertreter sehen hier Potenzial (Politiker: 100 Prozent). Grundsätzlich einig sind sich Politik und Wirtschaft also darin, dass der Staat dazu beitragen kann, die IT-Sicherheit von Unternehmen zu erhöhen. Beide gehen aber eher davon aus, dass die Möglichkeiten des Staates in diesem Feld begrenzt sind, auch wenn Politiker den Beitrag, den der Staat leisten kann, etwas höher veranschlagen als Wirtschaftsführer.

Begrenzte Kenntnisse – Verantwortung auf beiden Seiten

Rund die Hälfte der Politiker fühlt sich nicht gut informiert über die Bedürfnisse der Wirtschaft in Sachen IT-Sicherheit.

Nur rund jeder fünfte Abgeordnete weiß relativ gut darüber Bescheid, welche staatlichen Gremien, Organisationen und Einrichtungen sich in Deutschland mit dem Thema Cyber-Sicherheit beschäftigen, rund zwei Drittel haben einen groben Überblick und 15 Prozent haben sich damit noch gar nicht beschäftigt.

Informationen zum Thema IT-Sicherheit beziehen Abgeordnete vor allem aus ihrer jeweiligen Fraktion und von Behörden wie dem BSI. Für 81 Prozent sind diese Informationen alles in allem auch eine gute Entscheidungshilfe. Sind aber politische Beschlüsse zum Thema IT-Sicherheit zu treffen, räumen zwei Drittel der Abgeordneten ein, dass sie sich auf das verlassen müssen, was ihnen Experten raten. Sie sehen sich kaum in der Lage, sich eigenständig ein Urteil in diesem Feld zu bilden.

Andersherum sehen entsprechend auch nur 25 Prozent der Wirtschaftsführer die Cyber-Security-Bedürfnisse ihrer Unternehmen als vom Staat gut abgedeckt. Dabei bestehen allerdings auch bei Wirtschaftsentscheidern begrenzte Kenntnisse zu den staatlichen Gremien, Organisationen und Einrichtungen, die sich in Deutschland mit dem Thema Cyber-Sicherheit beschäftigen; nur 9 Prozent der Wirtschaftsführer insgesamt und 10 Prozent der Wirtschaftsführer mit Zuständigkeit für den IT-Bereich geben an, dass sie sich relativ gut damit auskennen. Auch Abgeordnete räumen mehrheitlich ein, dass die staatlichen Institutionen die Bedürfnisse der Wirtschaft im Feld der Cyber-Sicherheit ihrem Eindruck nach bislang nur weniger gut oder gar nicht gut abdecken. Hier besteht eine klare, gemeinsame Verantwortung zum Aufbau eines gegenseitigen Verständnisses auf beiden Seiten. Dies kann nur durch einen konstruktiven Austausch ermöglicht werden.

Abb. 16 – Informationsstand über IT-Sicherheit

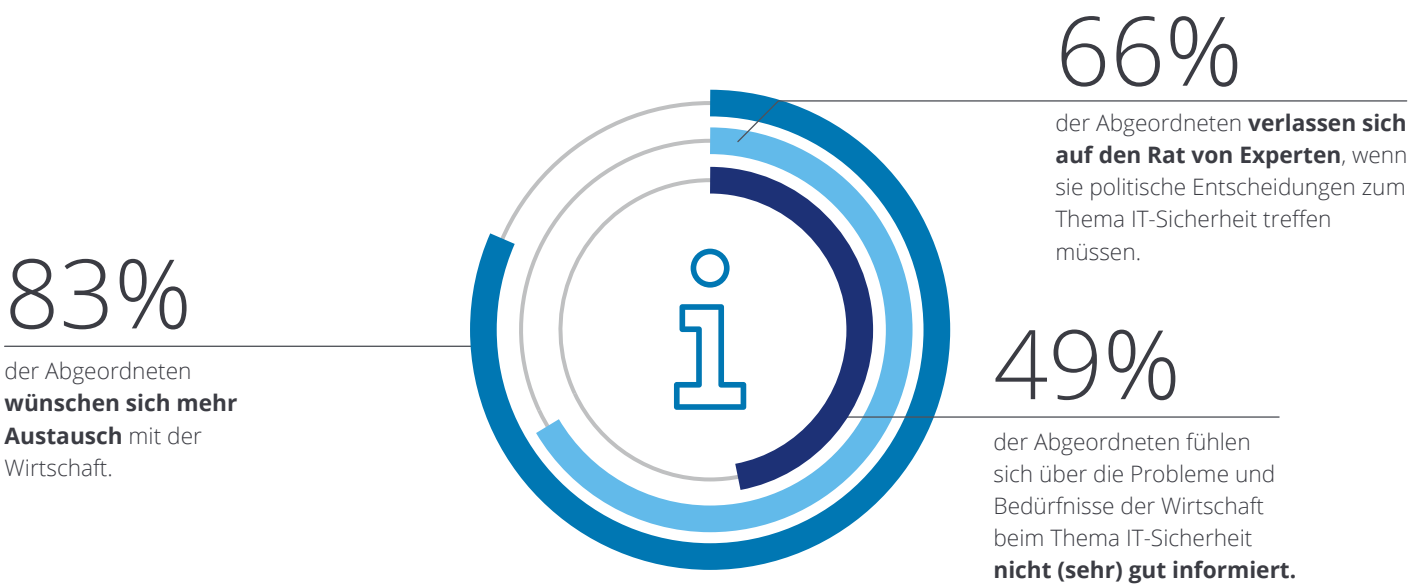
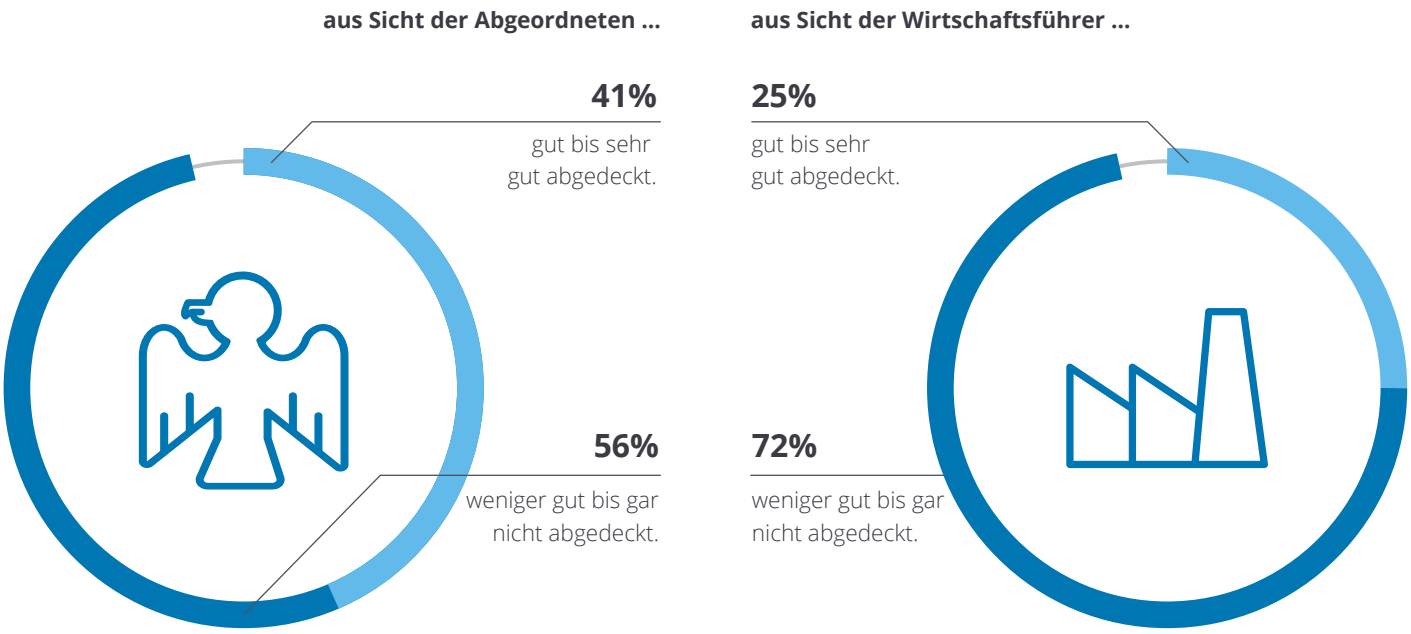


Abb. 17 – Deckung der IT-Sicherheitsbedürfnisse der Wirtschaft

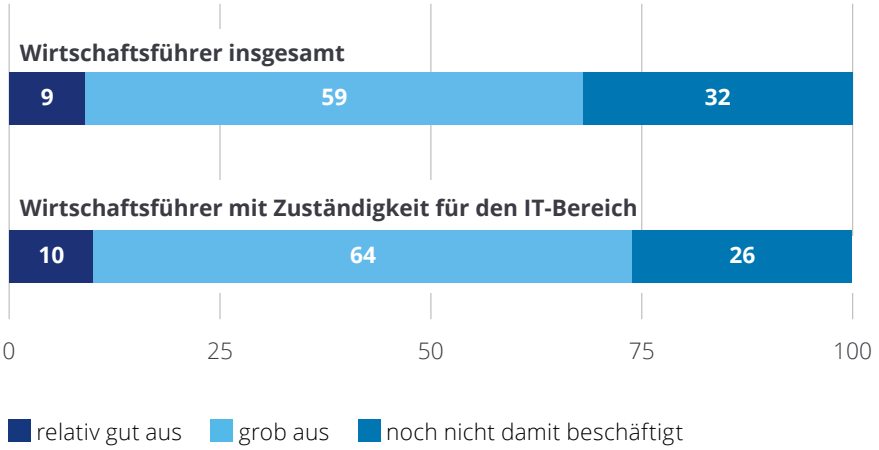
Die Bedürfnisse der Wirtschaft im Bereich Cyber-Sicherheit werden von den verschiedenen staatlichen Institutionen und Organisationen ...



Auf 100 fehlende Prozent: unentschieden

Abb. 18 – Wissen über staatliche Cyber-Sicherheitsorganisationen

Damit, welche staatlichen Gremien, Organisationen und Einrichtungen sich in Deutschland mit dem Thema Cyber-Sicherheit beschäftigen, kennen sich …



In Prozent der Nennungen.

Nachholbedarf beim Austausch

In diesem Rahmen beklagt eine deutliche Mehrheit sämtlicher Top-Entscheider einen mangelnden Austausch zwischen staatlichen Stellen und Privatwirtschaft (Abgeordnete: 83 Prozent, Wirtschaftsführer: 89 Prozent). Hier besteht offensichtlich noch ganz erheblicher Nachholbedarf. Dazu trägt vielleicht auch bei, dass das Zusammenspiel der diversen Behörden für außenstehende Beobachter derzeit nicht immer transparent wird. Ein gemeinsames Lagebild der verschiedenen öffentlichen Stellen sowie eine bundeseinheitliche Kontaktmöglichkeit, z.B. auch für einzelne Bürger in Sachen Sicherheit, könnten Schritte in die richtige Richtung darstellen.

Das Zusammenspiel von Staat und Wirtschaft ist maßgeblich für den Umgang mit den stetig wachsenden Cyber-Risiken. Unabdingbar dafür sind ein gutes gegenseitiges Verständnis von Politikern und Wirtschaftsentscheidern über Strukturen und Probleme. Obwohl hier grundsätzlich noch Ausbaubedarf besteht, werden die rechtlichen Rahmenbedingungen beispielsweise bereits als gute Grundlage gesehen.

5. Rahmenbedingungen für Standort

Gute Standortbedingungen bilden die Grundlage für unternehmerischen Erfolg, vor allem für eine stark exportorientierte Wirtschaft. Zu diesen Standortvorteilen zählen auch die rechtlichen Rahmenbedingungen für Cyber-Sicherheit. Die Bundesregierung sieht in diesen Rahmenbedingungen zur Cyber-Sicherheit auch ein neues Qualitätsmerkmal – Cyber Security made in Germany. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich hierfür das Ziel gesetzt, in ganz Deutschland ein einheitlich hohes IT-Sicherheitsniveau zu schaffen.[9] Dieser Abschnitt des Cyber Security Report zeigt die Wahrnehmung der Rahmenbedingungen in Deutschland durch die Befragten aus Wirtschaft und Politik.

Im Vergleich mit anderen Ländern bietet Deutschland gute rechtliche Grundlagen im Bereich IT-Sicherheit – so sieht es zumindest ein Großteil der befragten Führungskräfte und Abgeordneten. Alles in allem bewerten Wirtschaftsführer diese Gegebenheiten ganz überwiegend als gut (58 Prozent). Nur 11 Prozent haben den Eindruck, Deutschland biete hier eher schlechte Rahmenbedingungen, rund ein Viertel kann (oder will) das nicht beurteilen. Überdurchschnittlich positiv werden die rechtlichen Voraussetzungen im Bereich IT-Sicherheit in Deutschland von Führungskräften aus großen Unternehmen mit 1.000 und mehr Mitarbeitern bewertet.

Abb. 19 – Rechtliche Rahmenbedingungen in Deutschland

Im Vergleich mit anderen Ländern bietet Deutschland gute rechtliche Vorgaben im Bereich IT-Sicherheit.

[9] Bundesminister Horst Seehofer und BSI-Präsident Arne Schönbohm

Wie sich staatliche Rahmenbedingungen beziehungsweise Regulierung positiv auf Cyber-Sicherheit auswirkt, zeigt sich interessanterweise bei der im Sommer letzten Jahres so sehr als kompliziert und extrem bürokratisch gescholtenen Datenschutz-Grundverordnung: Die Einführung der DSGVO hat sich nach Einschätzung der Führungskräfte in rund der Hälfte der Unternehmen auf die IT-Sicherheit ausgewirkt. Diese Auswirkungen werden überwiegend als Verbesserung der IT-Sicherhiet bewertet, insbesondere in großen Unternehmen mit 1.000 und mehr Mitarbeitern.

Große Unternehmen sehen eher eine Verbesserung der IT-Sicherheit durch die Einführung der DSGVO.

Abb. 20 – IT-Sicherheitsgesetze und -verordnungen in Deutschland und der EU, in Kraft und im Entwurf

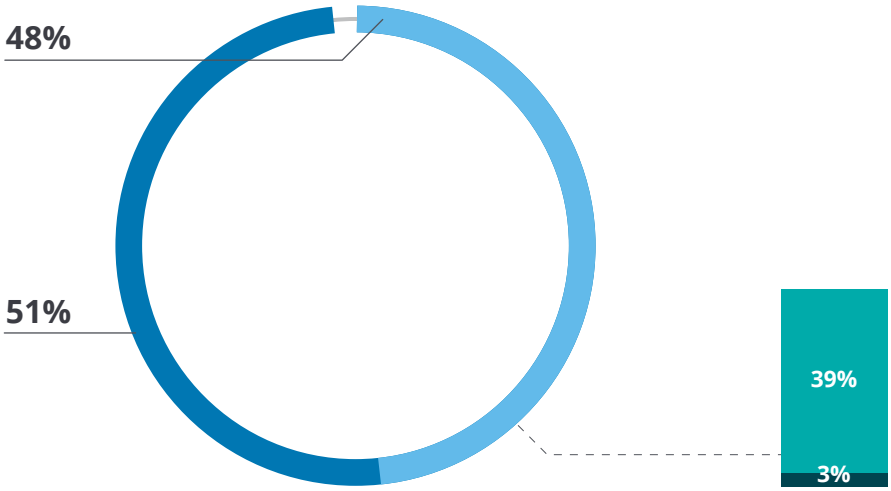
* Richtlinie des Europäischen Parlaments und des Rates über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung

Abb. 21 – Auswirkungen der DSGVO

Die Einführung der Datenschutzgrundverordnung hat sich auf die IT-Sicherheit im eigenen Unternehmen …

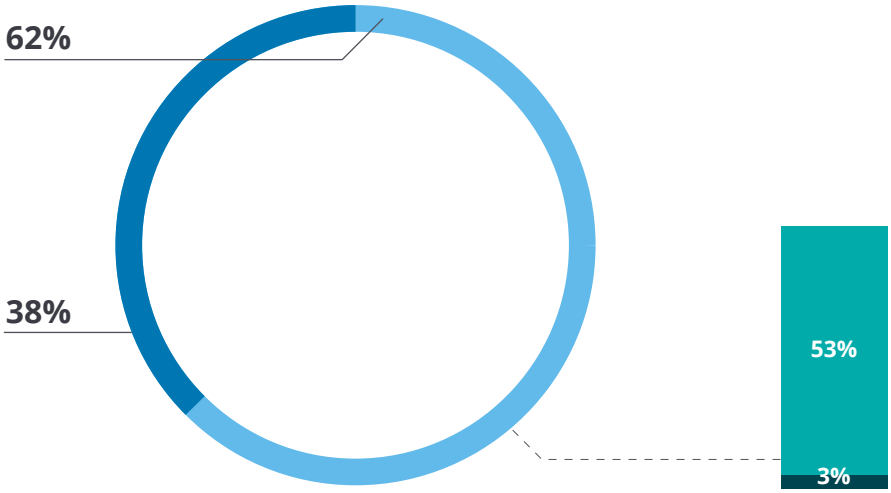
ausgewirkt nicht ausgewirkt

für die Führungskräfte insgesamt …



für die Führungskräfte aus Unternehmen mit 1.000 und mehr Mitarbeitern …

ausgewirkt nicht ausgewirkt



Die IT-Sicherheit hat sich dadurch alles in allem …

eher verbessert eher verschlechtert

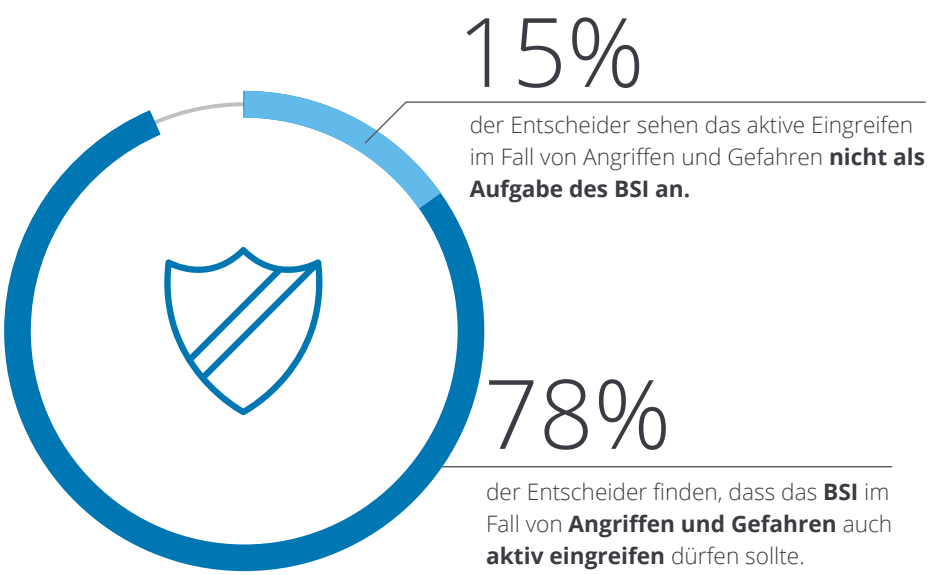
Auf 100 fehlende Prozent: unentschieden

In einigen Bereichen werden auch mehr Möglichkeiten staatlicher Institutionen gewünscht: Beispielsweise in Bezug auf die Aufgaben des BSI wünschen sich viele mehr Befugnisse für die Behörde. Eine mögliche Ausweitung der Kompetenzen des BSI von defensivem Schutz und Beratung hin zu einem aktiven Eingreifen im Falle von Angriffen und Gefahren trifft auf breite Zustimmung unter den Top-Entscheidern: Über drei Viertel sprechen sich dafür, nur 15 Prozent ausdrücklich dagegen aus.

Ein weiteres durch den Staat getriebenes Thema, das sich auf Unternehmen auswirkt, ist die Einstufung als Betreiber kritischer Infrastrukturen (KRITIS). Aktuell müssen Unternehmen in Deutschland anhand eines Kriterienkatalogs selbst überprüfen, ob sie zur KRITIS gehören, und sich beim BSI registrieren. So befürworten Politiker wie Wirtschaftsführer mehrheitlich, dass die Zuordnung von Unternehmen zur kritischen Infrastruktur nicht mehr von den Unternehmen selbst, sondern von einer unabhängigen Stelle vorgenommen werden sollte.

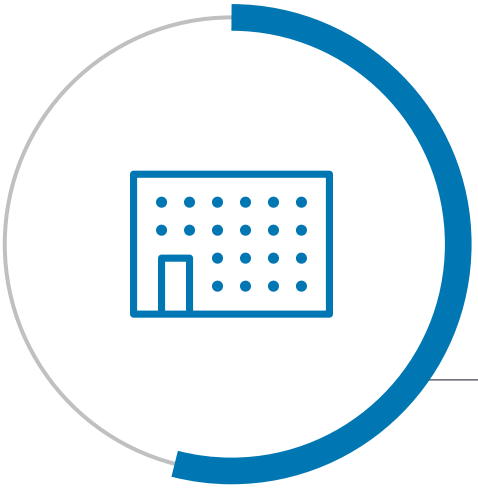
Auf noch breitere Zustimmung stößt der Vorschlag, für Unternehmen ab einer bestimmten Größe verbindlich einen Beauftragten für Cyber-Sicherheit vorzusehen, der bestimmte Kriterien erfüllen und sich regelmäßig fortbilden muss. Große Unternehmen votieren überdurchschnittlich häufig für diesen Vorschlag.

Abb. 22 – Breite Zustimmung zur aktiven Gefahrenbekämpfung



Auf 100 fehlende Prozent: unentschieden

Abb. 23 – Einstufung als KRITIS-Unternehmen



53%

der Entscheider bevorzugen eine **unabhängige Überprüfung,** ob ein Unternehmen zur **sogenannten „kritischen Infrastruktur" (KRITIS)** gehört.

Abb. 24 – Cyber-Sicherheitsbeauftragter

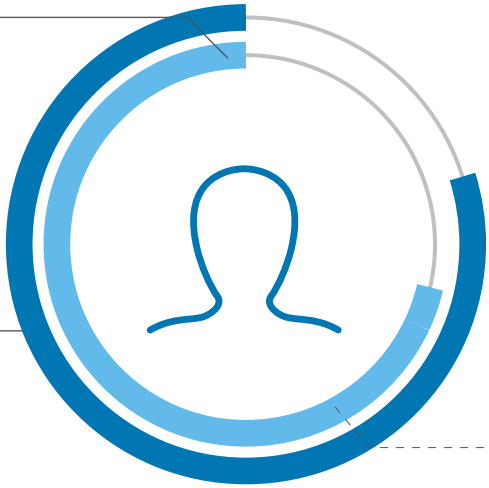
Ab einer bestimmten Größe sollte es in allen Unternehmen einen obligatorischen Beauftragten für Cyber-Sicherheit geben, der bestimmte Kriterien erfüllen und sich regelmäßig fortbilden muss.

68%

der **Wirtschaftsführer insgesamt** sehen das so.

77%

der **Abgeordneten** sehen das so.



82%

der **Wirtschaftsführer aus Unternehmen mit 1.000 und mehr Mitarbeitern** sehen das so.

Bei der Einschätzung der Relevanz nationaler Rahmenbedingungen fallen die Einschätzungen von Abgeordneten und Führungskräften unterschiedlich aus:

Nach Einschätzung von über drei Vierteln der Abgeordneten haben die nationalen Rahmenbedingungen im Bereich IT-Sicherheit auch große oder sehr große Bedeutung für die Entscheidung von Unternehmen, in welchen Ländern sie in bestimmte Technologien investieren.

Die Führungskräfte aus der Wirtschaft hingegen veranschlagen diese Bedeutung deutlich geringer. Hier berichten nur 27 Prozent von einem großen oder sehr großen Einfluss dieser Rahmenbedingungen auf die Investitionsentscheidungen ihrer Unternehmen. Allerdings ist rund ein Drittel der Unternehmen gar nicht in anderen Ländern aktiv oder die befragte Führungskraft in dieser Frage nicht auskunftsfähig.

Ähnlich groß ist die Bedeutung der genannten Rahmenbedingungen für die Entscheidung, wo Unternehmen Software oder Systeme entwickeln lassen bzw. von wo sie Software und Systeme beziehen: Bei einem knappen Drittel der Unternehmen spielen dafür die jeweiligen nationalen rechtlichen Regelungen im Bereich IT-Sicherheit eine große oder sehr große Rolle.

Deutlich größer ist dagegen der Einfluss bei der Auswahl von IT-Dienstleistern wie z.B. Cloud-Anbietern: Bei rund zwei Dritteln der Unternehmen spielen die nationalen Regelungen eine wichtige oder sehr wichtige Rolle, wenn es darum geht, mit Dienstleistern aus welchen Ländern man kooperiert.

Die deutsche Wirtschaft profitiert von einer vernetzten und digitalisierten Welt, der Staat und die Gesellschaft in derselben Weise. Gleichzeitig sind alle Bereiche des Lebens und Arbeitens gegen Cyber-Angriffe verwundbarer geworden. Cyber-Sicherheit ist eine gesamtstaatliche Aufgabe, die eine Zusammenarbeit über rechtliche Rahmenbedingungen hinaus erfordert.

Abb. 25 – Bedeutung nationaler Rahmenbedingungen aus Sicht der Abgeordneten

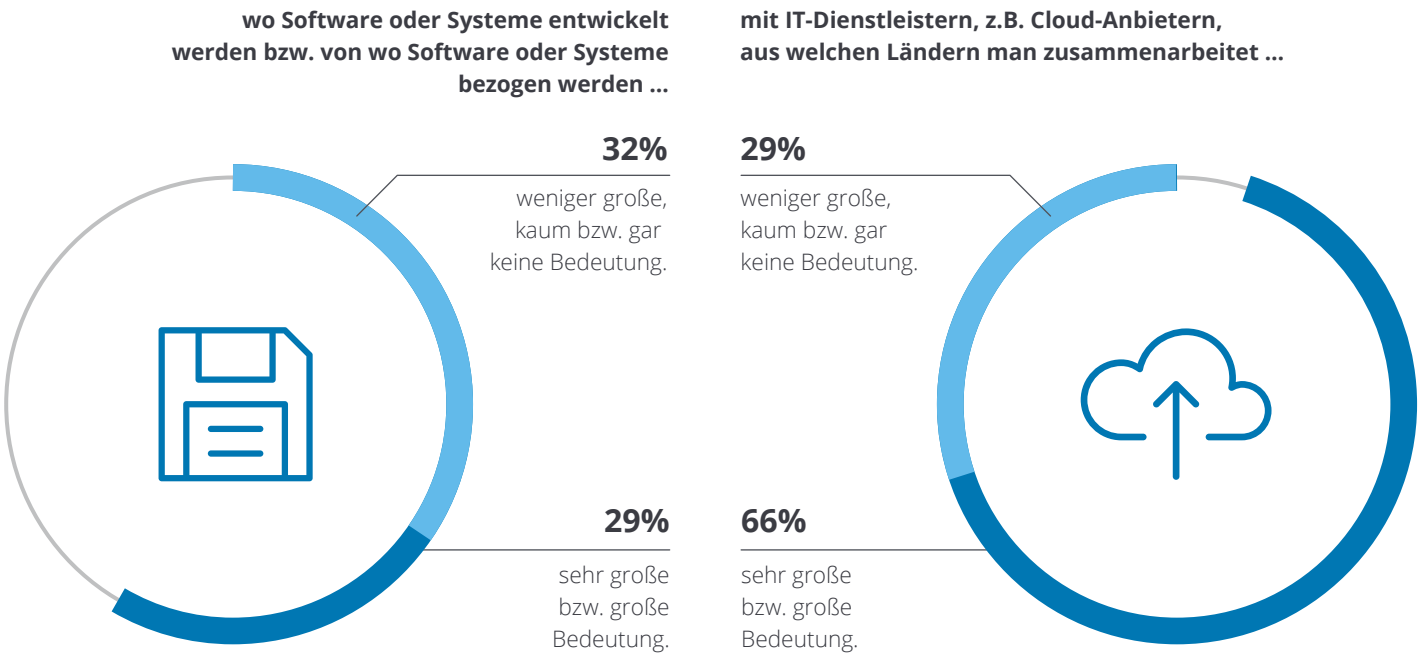
80%

der Abgeordneten sehen eine **große oder sehr große Bedeutung** in den **nationalen Rahmenbedingungen** im Bereich IT-Sicherheit für die Entscheidung von Unternehmen, **in welchen Ländern sie in bestimmte Technologien investieren.**

Nationale Rahmenbedingungen im Bereich IT-Sicherheit: Politiker sehen große Bedeutung für Investitionsentscheidungen von Unternehmen – Führungskräfte sind hier zurückhaltender.

Abb. 26 – Rahmenbedingungen und Investitionsentscheidungen

Die nationalen Rahmenbedingungen im Bereich IT-Sicherheit haben für die Entscheidung ...



Auf 100 fehlende Prozent: Sind nicht in anderen Ländern aktiv bzw. kennen die Rahmenbedingungen nicht

Handlungsfelder

Die erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft bedeutet auch, sich den sich dynamisch entwickelnden Anforderungen an die Cyber-Sicherheit zu stellen. Dies kann nur im Zusammenspiel aller Akteure gelingen.

Fake News und Meinungsbildung
Die erkannte Gefährdung sowohl des demokratischen Prozesses als auch der Reputation eines Unternehmens durch Meinungsmanipulation und Fake News erfordert fortlaufende Sensibilisierung, Überwachung und proaktives Management der Kommunikationskanäle durch staatliche Stellen, politische Akteure und die Unternehmen selbst. Dazu gehört zuallererst, im Blick zu haben, was über das eigene Unternehmen oder die Institution in den sozialen Medien berichtet wird. Wesentlich Informationen sollten hinterfragt werden; zur Verifikation können auch moderne Instrumente aus Data Analytics oder KI eingesetzt werden.

Ausbau der regulatorischen Rahmenbedingung für IT-Sicherheit
Die geschaffenen regulatorischen Rahmenbedingungen werden positiv eingeschätzt. Im Dialog mit der Wirtschaft müssen diese stetig wachsenden Anforderungen gemeinsam fortentwickelt und an den Fortgang in der Bedrohungslandschaft angepasst werden. Die Unternehmen erkennen die positive Wirkung der Regulierung und sind zum Dialog und zur Zusammenarbeit Staat und Wirtschaft bereit.

Sicherheitsrelevant: digitale Schlüsseltechnologien
Risiken werden in der großen Abhängigkeit von nicht-europäischen Anbietern für Schlüsseltechnologien gesehen. Die diesbezügliche Souveränität wird daher zur Voraussetzung für eine erfolgreiche und sichere Digitalisierung. Hier müssen Rahmenbedingungen für gefestigte europäische Technologieentwicklungen geschaffen werden.

Staat und Wirtschaft
Die grundsätzliche Einigkeit zwischen Politik und Wirtschaft darüber, dass der Staat dazu beitragen kann, die Informationssicherheit von Unternehmen zu erhöhen, sollte als Basis für einen intensiven Austausch genutzt werden. Staatliche Institutionen könnten die offenen Informationsbedürfnisse der Wirtschaft untersuchen und standardisierte Stakeholder-Dialoge etablieren. Der Dialog in der Umsetzung neuer regulatorischer Anforderungen sollte weiterhin aufrechterhalten bleiben.

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 09/2019