Deloitte.

Cyber Security Report 2019

Rahmenbedingungen für IT-Sicherheit

Vorwort

Cyber Security Report 2019
Vorwort

Die digitale Transformation verändert unaufhaltsam die Art und Weise, wie wir arbeiten und leben. Innovationen und Schlüssel-technologien 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.

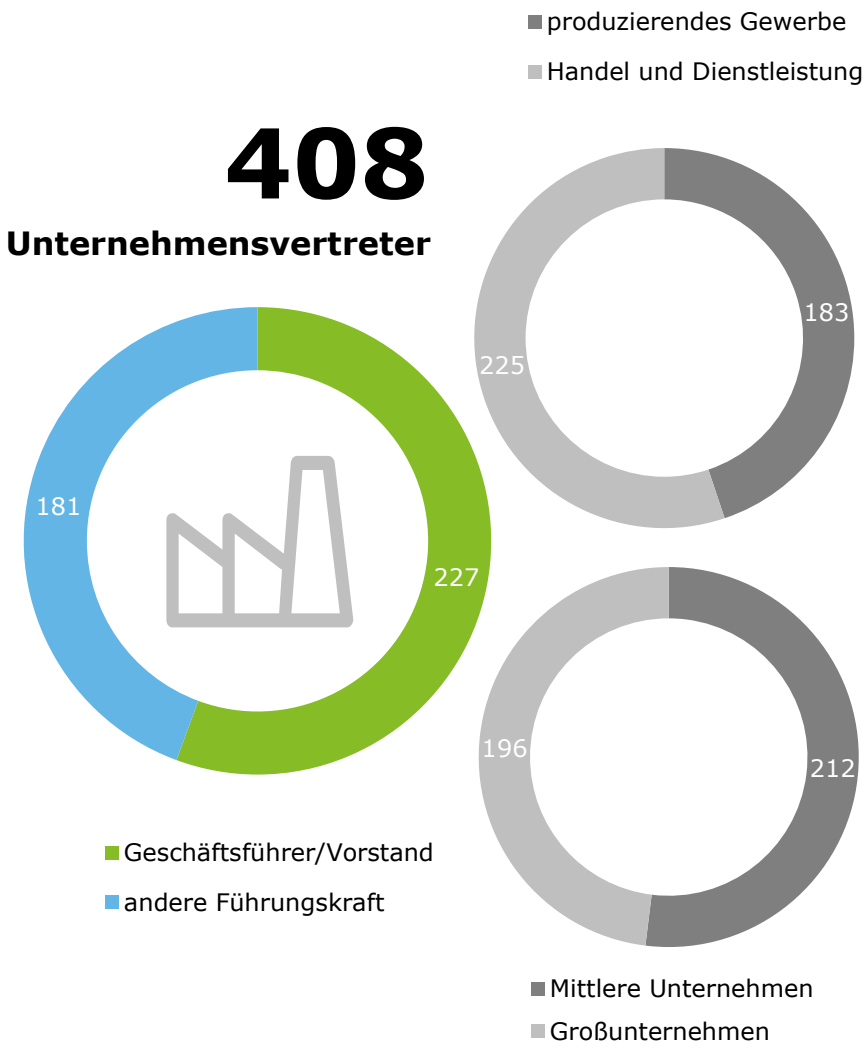
Wir haben im neunten Jahr in Folge in der Studie die Einschätzung der Bedrohung durch Cyber- und IT-Risiken und der daraus folgenden Gefahren für Staat und Unternehmen dargestellt. Politiker und Wirtschaftsführer geben Auskunft über die Zahl der erfolgten Angriffe, die Art der daraus folgenden Schäden und die von ihnen ergriffenen Maßnahmen.

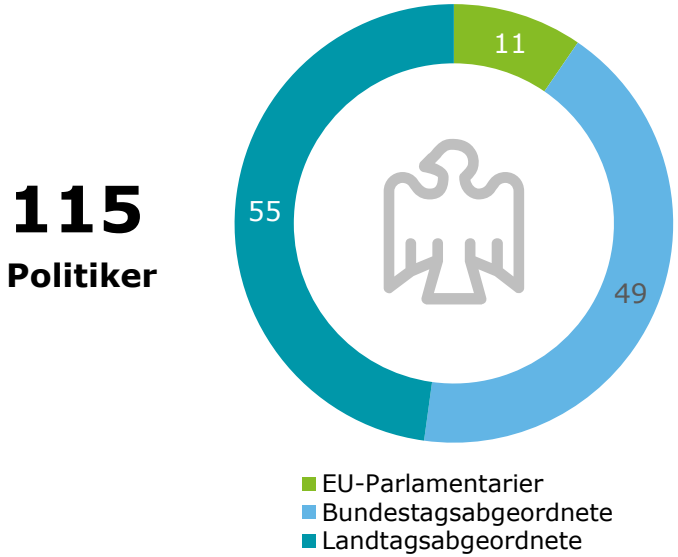
Wir haben den Fokus der Trendstudie in diesem Jahr um wesentliche Punkte der aktuellen Situation in den Unternehmen und wichtige Fragestellungen aus der gesellschaftlichen und politischen Debatte ergänzt:

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

Studiendesign

Cyber Security Report 2019
Studiendesign





Stichprobe

Als Großunternehmen gelten gemäß der Definition der EU-Kommission Unternehmen mit mindestens 250 Beschäftigten und/oder mehr als 50 Mio. Euro Jahresumsatz. Mittlere Unternehmen sind gemäß Definition der EU-Kommission Unternehmen, die zwischen 50 und 249 Mitarbeiter haben und/oder einen Jahresumsatz von 10 bis höchstens 50 Mio. Euro erzielen.

Methode

Telefonische Interviews (CATI)

Befragungszeitraum

26. Juni bis 8. August 2019

Kernaussagen

Cyber Security Report 2019
Kernaussagen

Meinungsmanipulation und Fake News sind höchstes Risiko

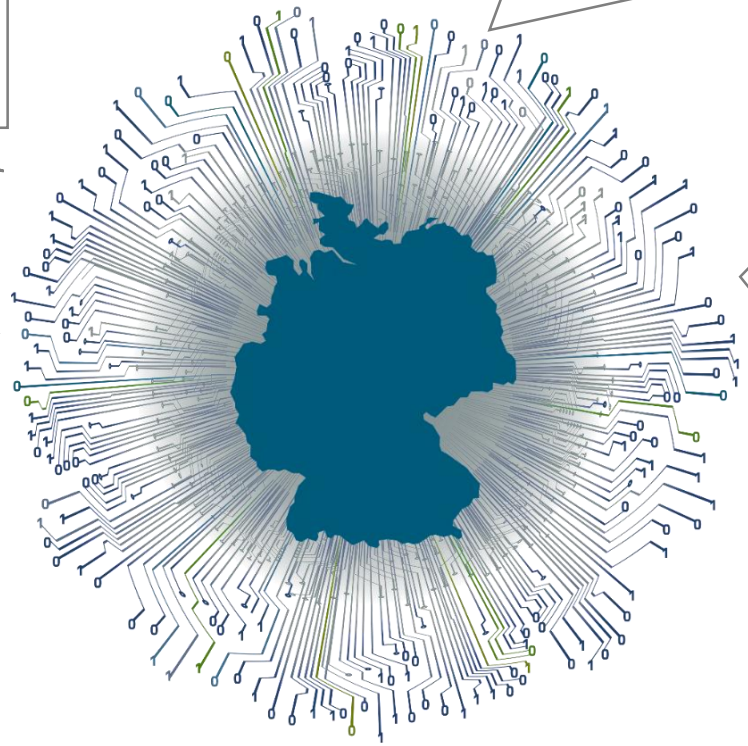
Deutliche Mehrheiten der Entscheidungsträger stufen Cyber-Gefahren als hohes Risiko ein. Befragte aus der Wirtschaft bewerten die Risiken dabei höher als Abgeordnete. Die Manipulation der öffentlichen Meinung, z.B. durch Fake News belegt dabei erstmals den Spitzenplatz des Rankings. Die Hälfte der Politiker erkennt im steigenden Einfluss der sozialen Medien eine Gefahr für die Demokratie, die jeweils eigene Partei überwiegend Chancen.

Industrie 4.0 auf dem Vormarsch – aber die Sicherheit?

Die Zahl der Führungskräfte in der Wirtschaft, die sich schon intensiv mit Industrie 4.0 beschäftigt hat, steigt stetig. Eine Mehrheit hält es für eher sicher, zur Vernetzung der Produktionsabläufe den 5G-Standard nutzen zu wollen. Dass sich hieraus deutliche Veränderungen für die Cyber-Security-Strategie des Unternehmens ergeben, berichten allerdings nur 28 Prozent.

Gute Rahmenbedingungen für die IT-Sicherheit in Deutschland

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



Fehlende Unabhängigkeit bei Schlüsseltechnologien – Gefahr für die Cyber-Sicherheit?

Eine europäische Unabhängigkeit bei der Entwicklung von Schlüssel-technologien gilt für 89 Prozent der Abgeordneten und 71 Prozent der 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 den 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 gut 2/3 der Wirtschaftsvertreter die Bedürfnisse der Wirtschaft in diesem Bereich nicht gut durch staatliche Institutionen abgedeckt. Die Hälfte der Abgeordneten hingegen fühlen 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.

Cyber Security Report 2019

Meinungsmanipulation und Fake News sind höchstes Risiko

Deutliche Mehrheiten der Entscheidungsträger stufen Cyber-Gefahren als hohes Risiko ein. Befragte aus der Wirtschaft bewerten die Risiken dabei höher als Abgeordnete. Die Manipulation der öffentlichen Meinung, z.B. durch Fake News, belegt dabei erstmals den Spitzenplatz des Rankings. Die Hälfte der Politiker erkennt im steigenden Einfluss der sozialen Medien eine Gefahr für die Demokratie, die jeweils eigene Partei überwiegend Chancen.

25%

der Unternehmen berichten von Versuchen, den Ruf des Unternehmens durch **gezielte Falschinformationen im Internet** zu schädigen.

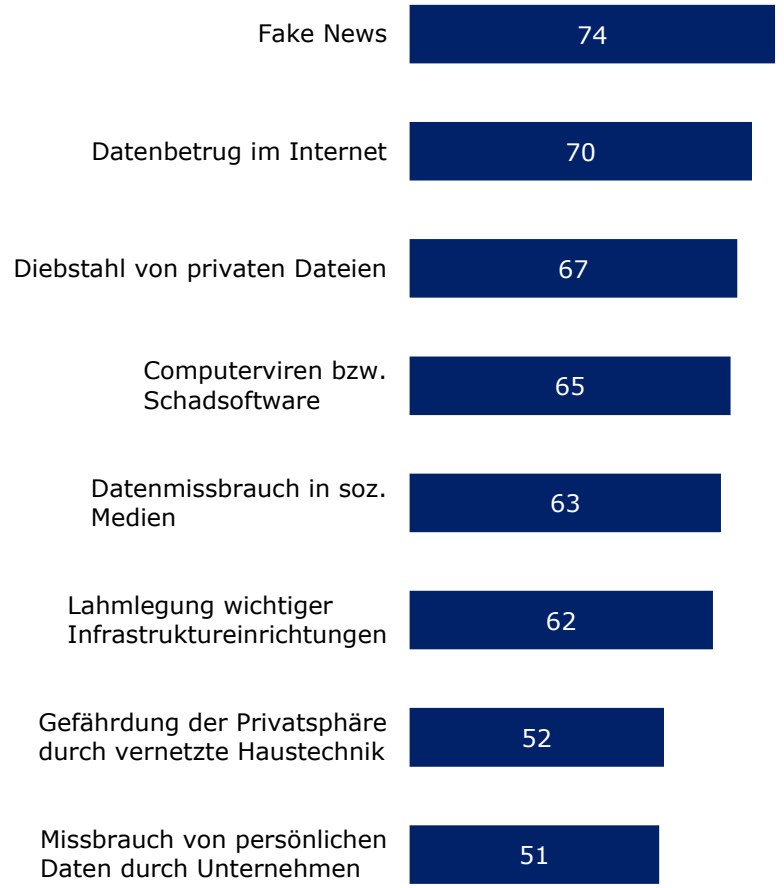
50%

der Abgeordneten sehen **eher Risiken** im steigenden Einfluss sozialer Medien auf die politische Meinungsbildung für die Demokratie in Deutschland.

34%

der Abgeordneten **sehen eher Chancen** im steigenden Einfluss sozialer Medien auf die politische Meinungsbildung für die Demokratie in Deutschland.

Wichtigste Risiken für die Menschen in Deutschland



In Prozent der Nennungen

Cyber Security Report 2019

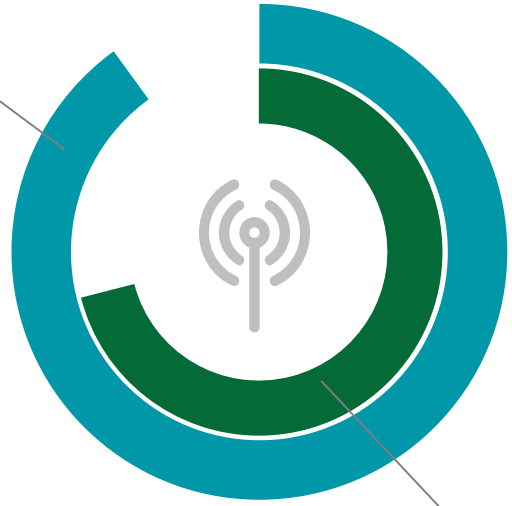
Fehlende Unabhängigkeit bei Schlüsseltechnologien – Gefahr für die Cyber-Sicherheit?

Eine europäische Unabhängigkeit bei der Entwicklung von Schlüsseltechnologien gilt für 89 Prozent der Abgeordneten und 71 Prozent der 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 den Befragten als große Gefahr bewertet.

89%

der Abgeordneten sehen das so.

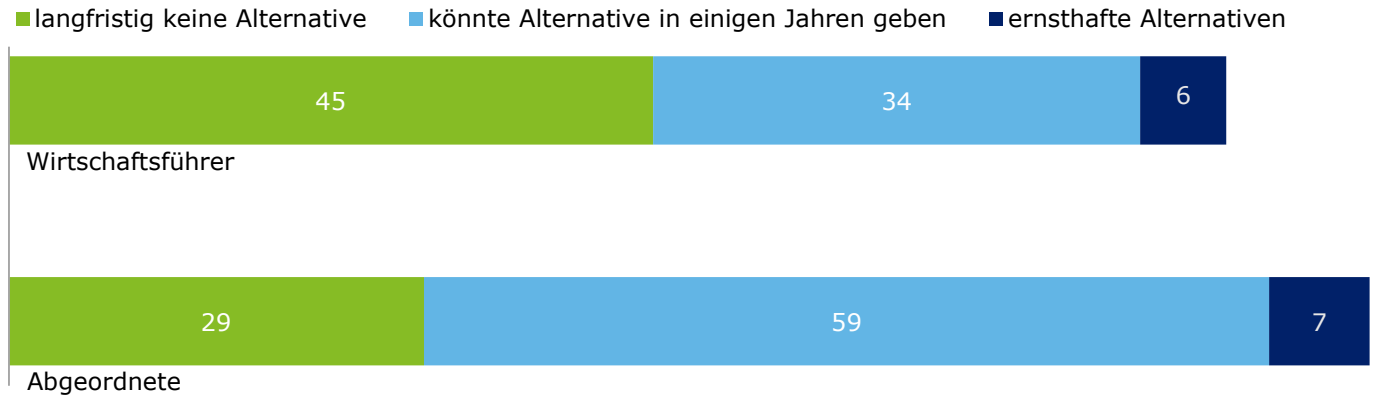
Um eine ausreichende Cyber-Sicherheit in Deutschland zu gewährleisten, müssen wichtige **Schlüsseltechnologien** für die Digitalisierung und Vernetzung **von deutschen oder europäischen Unternehmen** hergestellt werden.



71%

der Wirtschaftsführer sehen das so.

Bei Aufbau des 5G-Netzes hat Deutschland zu Technologien aus den USA und China…



Auf 100 fehlende Prozent: unentschieden.

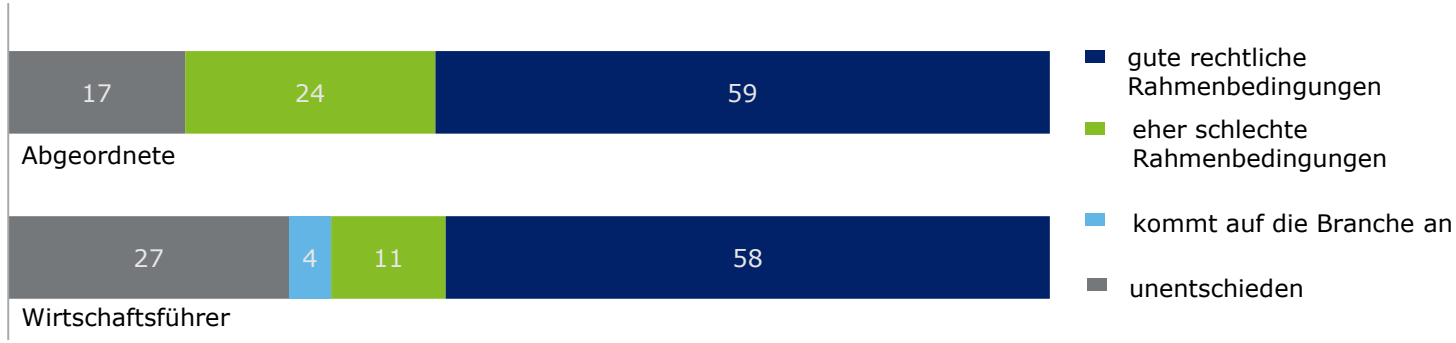
In Prozent der Nennungen.

Cyber Security Report 2019

Gute Rahmenbedingungen für die IT-Sicherheit in Deutschland

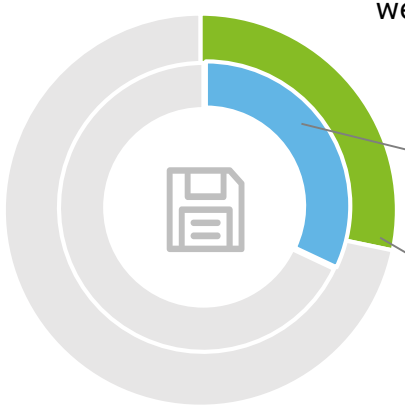
Die rechtlichen Rahmenbedingungen für IT-Sicherheit werden für Deutschland, verglichen mit anderen Ländern, positiv eingeschätzt. Insbesondere Vertreter größerer Unternehmen urteilen hier sehr positiv. Die Rahmenbedingungen beeinflussen Standortentscheidungen kaum. Lediglich bei der Auswahl von IT-Dienstleister, wie bspw. Cloud, ist der Standort sehr relevant.

Bietet Deutschland Unternehmen vergleichsweise zu anderen Ländern gute oder eher schlechte Rahmenbedingungen im Bereich IT-Sicherheit?



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

wo Software oder Systeme entwickelt werden bzw. von wo Software oder Systeme bezogen werden…



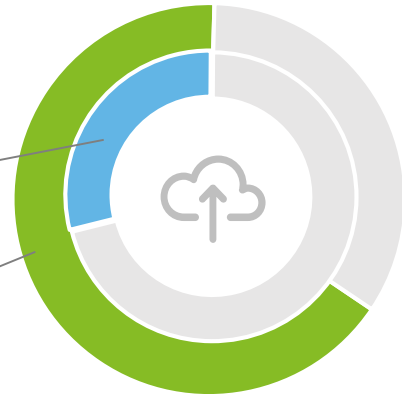
weniger große, kaum bzw. gar keine Bedeutung. 32%

sehr große bzw. große Bedeutung. 29%

mit IT-Dienstleistern, z.B. Cloud-Anbietern, aus welchen Ländern man zusammenarbeitet…

29% weniger große, kaum bzw. gar keine Bedeutung.

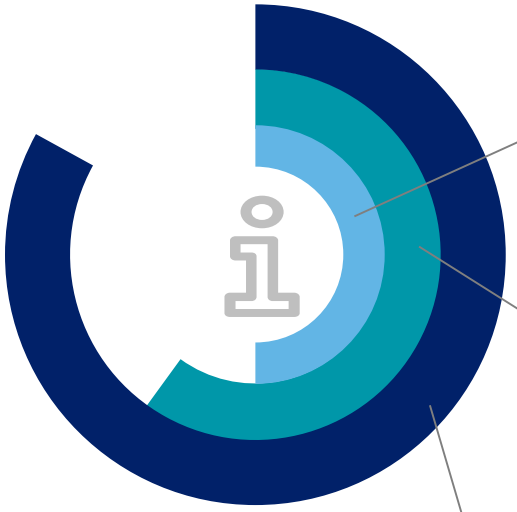
66% sehr große bzw. große Bedeutung.



In Prozent der Nennungen.

Cyber Security Report 2019
Staat und Wirtschaft

Die Politik kann zur Erhöhung der IT-Sicherheit in Unternehmen beitragen, davon sind Politiker und Wirtschaftsvertreter überzeugt. Allerdings sehen derzeit gut 2/3 der Wirtschaftsvertreter die Bedürfnisse der Wirtschaft in diesem Bereich nicht gut durch staatliche Institutionen abgedeckt. Die Hälfte der Abgeordneten hingegen fühlen 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.



49%

der Abgeordneten fühlen sich über die Probleme und Bedürfnisse der Wirtschaft beim Thema IT-Sicherheit **nicht (sehr) gut informiert.**

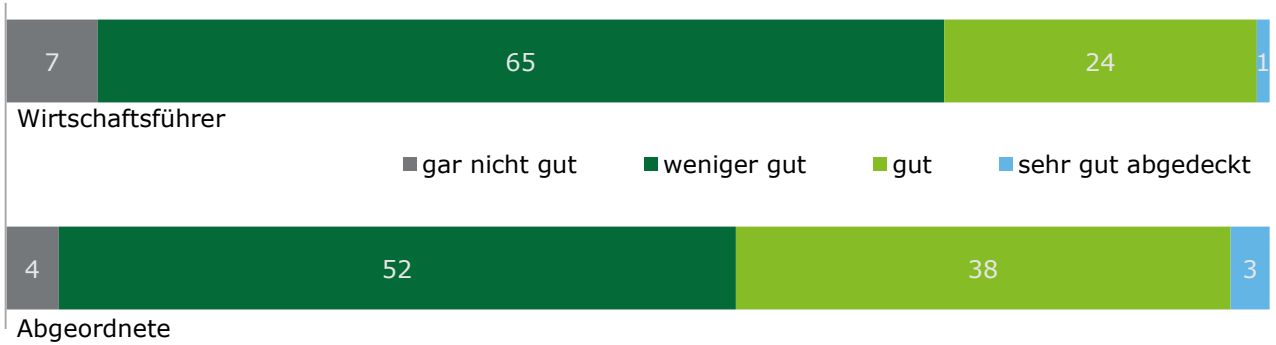
66%

der Abgeordneten **verlassen sich auf den Rat von Experten**, wenn sie politische Entscheidungen zum Thema IT-Sicherheit treffen müssen.

83%

der Abgeordneten **wünschen sich mehr Austausch** mit der Wirtschaft.

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



Auf 100 fehlende Prozent: unentschieden.

Cyber Security Report 2019

Industrie 4.0 auf dem Vormarsch – aber die Sicherheit?

Die Zahl der Führungskräfte in der Wirtschaft, die sich schon intensiv mit Industrie 4.0 beschäftigt hat, steigt stetig. Eine Mehrheit hält es für eher sicher, zur Vernetzung der Produktionsabläufe den 5G-Standard nutzen zu wollen. Dass sich hieraus deutliche Veränderungen für die Cyber-Security-Strategie des Unternehmens ergeben, berichten allerdings nur 28 Prozent.

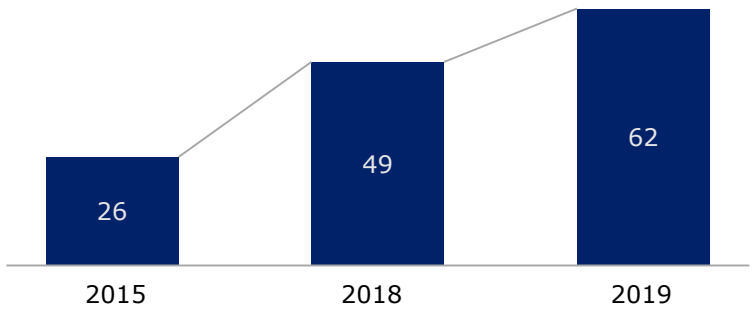
90%

der Führungskräfte, die sich mit dem Thema Industrie 4.0 schon (sehr) intensiv beschäftigt haben, halten **Industrie 4.0** für das eigene Unternehmen für **(sehr) wichtig**.

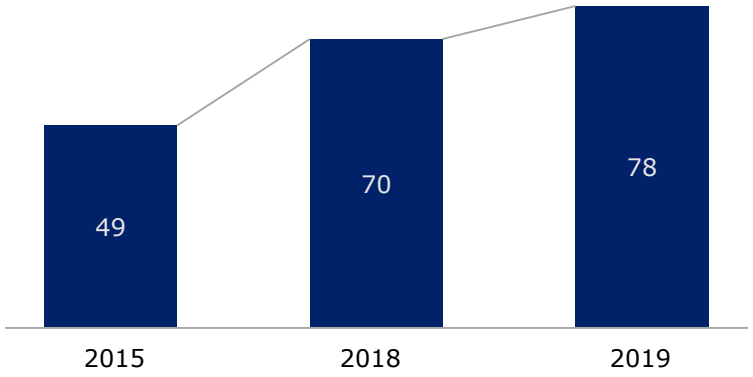
28%

der Führungskräfte, die sich schon (sehr) intensiv mit dem Thema befasst haben, berichten von deutlichen **Anpassungsbedarfen für Cyber-Security-Strategien** durch die Umstellung auf Industrie 4.0.

Mehr als die Hälfte der Führungskräfte im produzierenden Gewerbe haben sich schon **(sehr) intensiv mit „Industrie 4.0" beschäftigt.**



Die Mehrheit der Führungskräfte im produzierenden Gewerbe hält **„Industrie 4.0" für die Zukunft des eigenen Unternehmens für (sehr) wichtig.**



In Prozent der Nennungen.

Handlungsfelder

Cyber Security Report 2019
Handlungsfelder

01

Fake News und Meinungsbildung

Sowohl die erkannte Gefährdung des demokratischen Prozesses als auch der Reputation eines Unternehmens durch Meinungsmanipulation und Fake News erfordern fortlaufende Sensibilisierung, Überwachung und proaktives Management der Kommunikationskanäle durch staatliche Stellen, politische Akteure und die Unternehmen selbst.

02

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 die Entwicklungen in der Bedrohungslandschaft angepasst werden.

03

Sicherheitsrelevant: Digitale Schlüsseltechnologien

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

04

Industrie 4.0 und 5G

Durch den Einsatz von 5G-Technologien, zum Beispiel bei der Vernetzung von Produktionsanlagen, entstehen naturgemäß neue Angriffsvektoren. Industrie 4.0 erfordert deshalb besondere Sicherheitsanforderungen. Diese müssen stärker als bisher in den Cyber-Sicherheits-Strategien berücksichtigt und nachhaltig verfolgt werden.

05

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.

Gesprächspartner

Cyber Security Report 2019
Ihre Gesprächspartner

Katrin Rohmann

Government & Public Services
Industry Leader

krohmann@deloitte.de

+49 30 25468127

Kurfürstendamm 23
10719 Berlin
Deutschland

Peter J. Wirnsperger

Cyber Risk Leader

pwirnsperger@deloitte.de

+49 40 320804675

Dammtorstraße 12
20354 Hamburg
Deutschland

Deloitte.