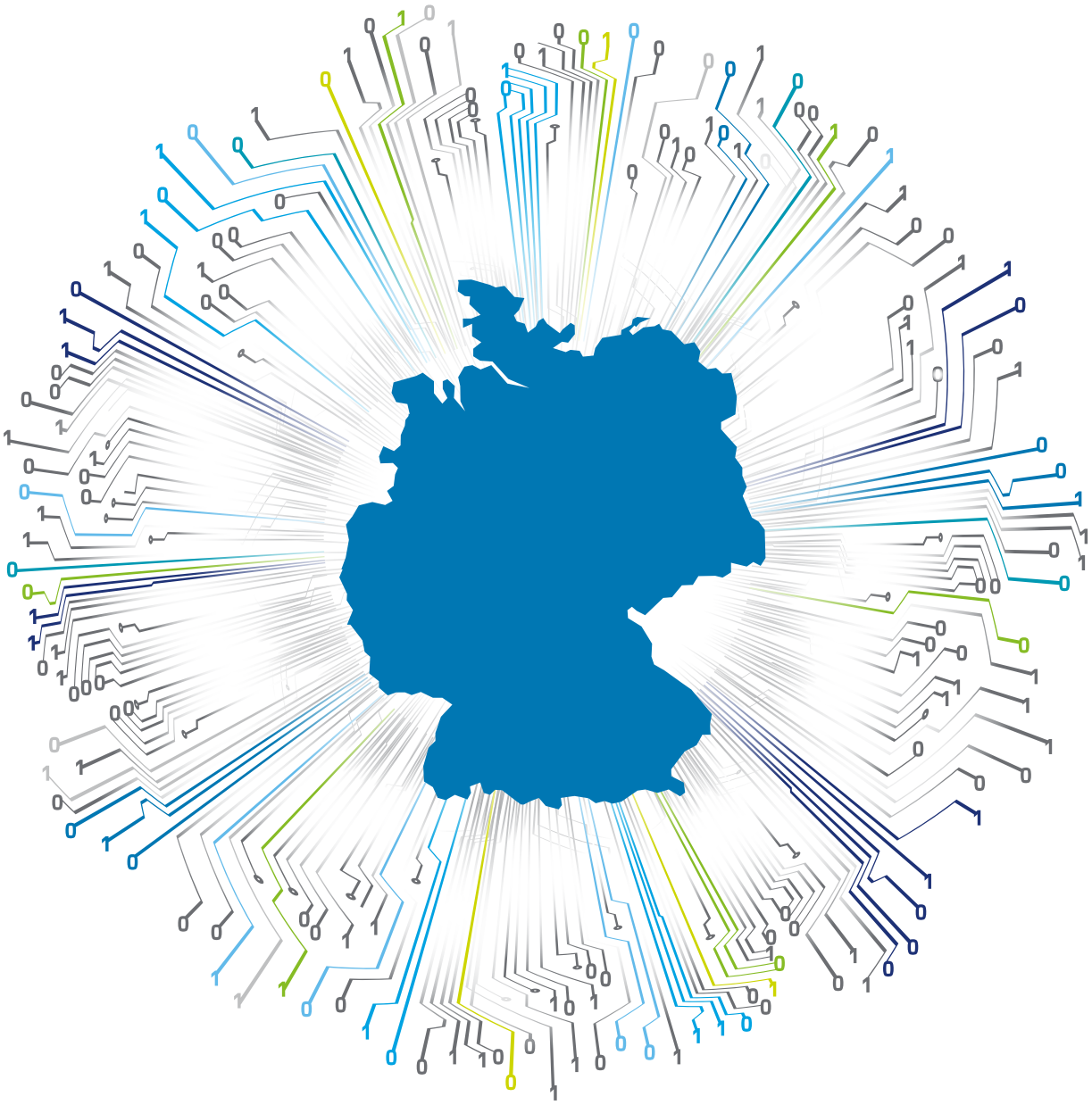
Deloitte.



Cyber Security Report 2018

Teil 2: Unternehmen – das Risikobewusstsein sinkt

Vorwort 04

Executive Summary 05

1. Sinkendes Bewusstsein für das Risiko 06

2. Differenzierte Sicht auf die potenziellen Schäden 10

3. Verantwortung und Kompetenz im Unternehmen 13

4. Schutz des Unternehmens 15

    4.1 Kosten 15

    4.2 Maßnahmen 18

    4.3 Sicherheit erfordert Kooperation 22

Handlungsfelder 25

Ansprechpartner 26

Vorwort

Die Chancen der Digitalisierung für die öffentliche Verwaltung und die Wirtschaft sind immens, die Risiken sind es ebenso. Größere Angriffswellen mit Ransomware sind im zurückliegenden Jahr ausgeblieben, doch die Bedrohungslage bleibt weiterhin kritisch.

Cyber-Angriffe gehören mittlerweile zum Alltag vieler Unternehmen und knapp die Hälfte der Studienteilnehmer wird sogar täglich bis mehrmals die Woche durch Cyber-Angriffe ausspioniert oder gar geschädigt. Ein Großteil der Befragten bemerkt den Angriff erst spät oder gar nicht.

Jedes Unternehmen stellt ein mögliches Angriffsziel dar. Einige sind gut vorbereitet, andere haben noch Nachholbedarf in Sachen Cyber-Sicherheit. Der Diebstahl von Know-how, der Imageverlust, die Umsatzeinbußen und die Kosten für die Behebung von Schäden durch Cyber-Attacken wirken sich unmittelbar auf den Wettbewerbsvorteil des Unternehmens aus. Cyber-Sicherheit stellt damit einen Wettbewerbsvorteil in der Digitalisierung dar und sollte eine strategische Aufgabe jeder Unternehmensführung sein.

Bei der Umsetzung von Unternehmensstrategien sind auch die Cyber-Risiken im Auge zu behalten. Insbesondere die Geschäftsführung ist gefragt, passende Strategien zu entwickeln, die Bewertung von Cyber-Risiken zu veranlassen und geeignete Schutzmaßnahmen umzusetzen. Vor dem Hintergrund, dass Cyber-Sicherheit bei der Umsetzung von Unternehmensstrategien eine hohe Priorität zukommen sollte, haben wir in diesem Teil des Reports folgende Planungsaspekte her ausgearbeitet:

Maßnahmen zur Erhöhung der Cyber-Sicherheit

Wir fragten die Führungskräfte, welche technischen und nicht-technischen Schutzmaßnahmen sie zur Erhöhung ihrer Cyber-Sicherheit ergreifen. Die Bandbreite an möglichen Vorkehrungen ist groß, sie reicht von einer laufenden Überwachung der Netzwerke über regelmäßige Überprüfungen der Zugriffsrechte bis hin zur Simulation von Cyber-Angriffen. Nur ein geringer Teil deutscher Unternehmen ist in der Lage, die gesamte Bandbreite an Maßnahmen selbst umzusetzen.

Kosten

Genauer hinterfragt haben wir auch, wie sich die Kosten für IT-Sicherheit, insbesondere für den Schutz vor Hacker-Angriffen, in den letzten Jahren entwickelt haben. Die Verantwortlichen sollten ermitteln, inwieweit der finanzielle Aufwand für die Abwehr einer Cyber-Bedrohung gerechtfertigt ist. Ein proaktives Anpassen von Cyber-Security-Maßnahmen oder ein Auslagern von kompletten Cyber-Security-Prozessen kann Kosten einsparen, Ressourcen freisetzen und dem Unternehmen helfen, sich auf sein Kerngeschäft zu konzentrieren.

Kooperationen

Cyber-Sicherheit fängt nicht erst am Werkstor an. Sie ist nicht nur Teil der unternehmensinternen Prozesse zur Wertschöpfung, sondern auch innerhalb der gesamten Wertschöpfungskette von Anfang bis Ende nachhaltig zu berücksichtigen. Deshalb fragten wir die Führungskräfte, ob sie ihre Lieferanten zur Einhaltung bestimmter IT-Sicherheitsstandards verpflichten.

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

Wie in den Vorjahren bildet die Einschätzung der Bedrohung durch Cyber- und IT-Risiken und der daraus folgenden Gefahren für Unternehmen den Schwerpunkt unserer Studie. Die Unternehmen geben auch Auskunft über die Zahl der erfolgten Angriffe und die Art der daraus resultierenden Schäden.

In Kooperation mit dem Institut für Demoskopie Allensbach haben wir diese repräsentative Umfrage unter Führungskräften der Wirtschaft und Politikern der Europa-, Bundes- sowie Landesparlamente durchgeführt.

Executive Summary

Die Ergebnisse der Befragung führen zu den folgenden Kernaussagen:

Sinkendes Risikobewusstsein und mangelnde Befassung mit Cyber-Sicherheit
Das Risikobewusstsein unter den Top-Entscheidern der Wirtschaft ist im Vergleich zum Vorjahr erneut gesunken. Geschäftsleitungen beschäftigen sich kaum oder nur sporadisch mit Cyber-Sicherheit und Aufsichtsräte legen nur in etwa der Hälfte der Fälle Wert auf regelmäßige Informationen zu dem Thema.

Unterschiedliche Wahrnehmung der Gefahren
Sowohl Wirtschaftsführer als auch Abgeordnete sehen das größte Risiko für die deutsche Wirtschaft insgesamt im Diebstahl von Know-how. Für das jeweils eigene Unternehmen bewerten Führungskräfte das deutlich anders. Am häufigsten halten sie die Kosten, die durch die Behebung von Schäden entstehen, für die größte Gefahr, die für ihr Unternehmen von Cyber-Angriffen ausgeht.

Überdurchschnittlich steigende Kosten
Grundsätzlich berichtet die überwiegende Mehrheit der Führungskräfte aus mittleren und großen Unternehmen, dass die Kosten für IT-Sicherheit in ihrem Unternehmen gestiegen sind. Überdurchschnittlich häufig haben solche ab 250 Mitarbeitern deutliche Kostensteigerungen zu verzeichnen.

Nicht alle Möglichkeiten zum Schutz werden genutzt
Zum Schutz ihrer IT-Infrastruktur ergreifen viele Unternehmen zwar eine Reihe von Maßnahmen, aber nur ein kleiner Teil schöpft die Möglichkeiten aus, die eigene Sicherheit im IT-Bereich zu optimieren. Eine Identifizierung der wichtigsten Information-Assets haben lediglich rund zwei Drittel der Befragten vorgenommen. Planspiele zur Simulation von Cyber-Angriffen, zum Beispiel War Games oder Red Teaming, führen gerade einmal 14 Prozent der Unternehmen regelmäßig durch. Eine Cyber-Versicherung besitzt nur knapp ein Viertel der Studienteilnehmer.

1. Sinkendes Bewusstsein für das Risiko

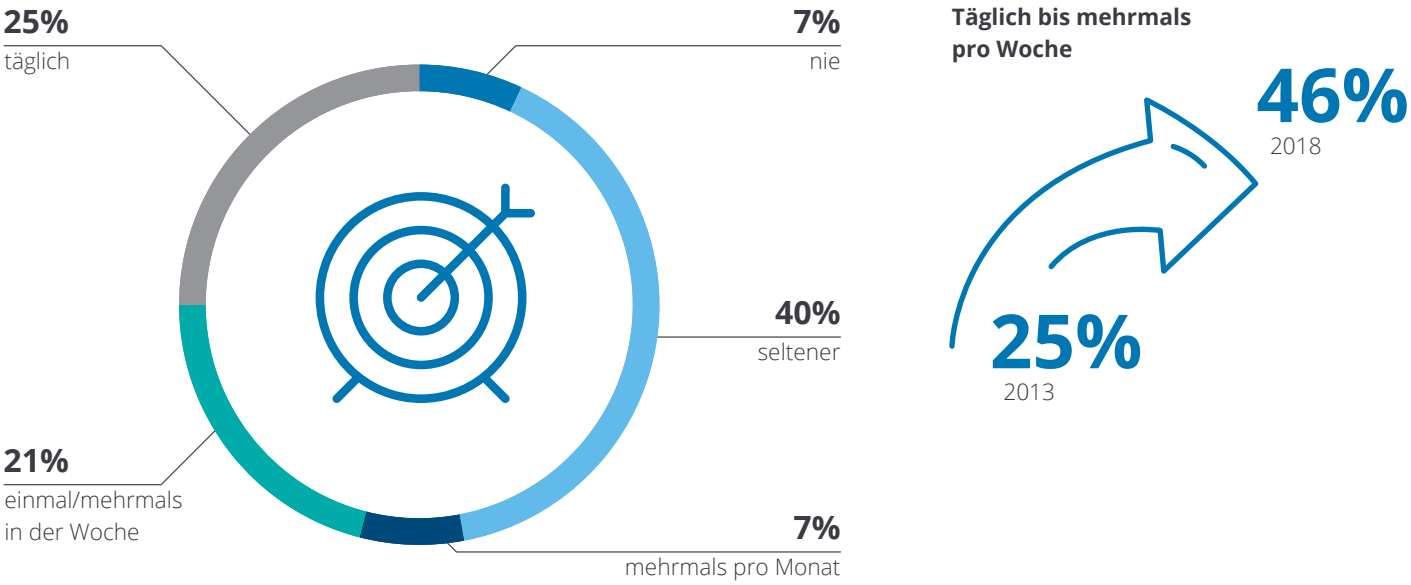
Cyber-Angriffe und -Kriminalität werden mittlerweile von der Gesellschaft, der Politik und der Wirtschaft als bekannte Phänomene wahrgenommen. Besonders mit WannaCry, der Ransomware-Attacke auf zahlreiche deutsche Unternehmen, mit dem APT-Angriff auf das Auswärtige Amt und dem Datenmissbrauch über Facebook durch Cambridge Analytica setzten sich die Medien stärker auseinander. Sie erhöhten damit auch die Wahrnehmung von Cyber-Risiken in Deutschland.

Für den Großteil der deutschen Unternehmen gehören Cyber-Angriffe zum Alltag. Insgesamt 93 Prozent der Befragten aus mittleren und großen Unternehmen bestätigten, IT-Angriffen ausgesetzt zu sein, durch die das Unternehmen ausspioniert oder geschädigt werden sollte. 25 Prozent der Befragten berichten von täglichen Angriffen, weitere 21 Prozent haben ein- oder mehrmals pro Woche mit externen Angriffen zu kämpfen, 7 Prozent mehrmals im Monat.

Das bestätigt auch die aktuelle Lagebeurteilung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Im Lagebericht vom 11. Oktober 2018 wird festgehalten, dass die Gefährdungslage weiterhin hoch, im Vergleich zum Vorjahr keinesfalls zurückgegangen und gleichzeitig auch noch vielschichtiger geworden ist.[1]

Abb. 1 – Wahrgenommene Häufigkeit von IT-Angriffen auf Unternehmen in Deutschland

Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt,
durch die Ihr Unternehmen ausspioniert oder geschädigt werden soll?



Nur Unternehmen, die eine konkrete Angabe gemacht haben.

[1] Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit 2018, S. 91 f.

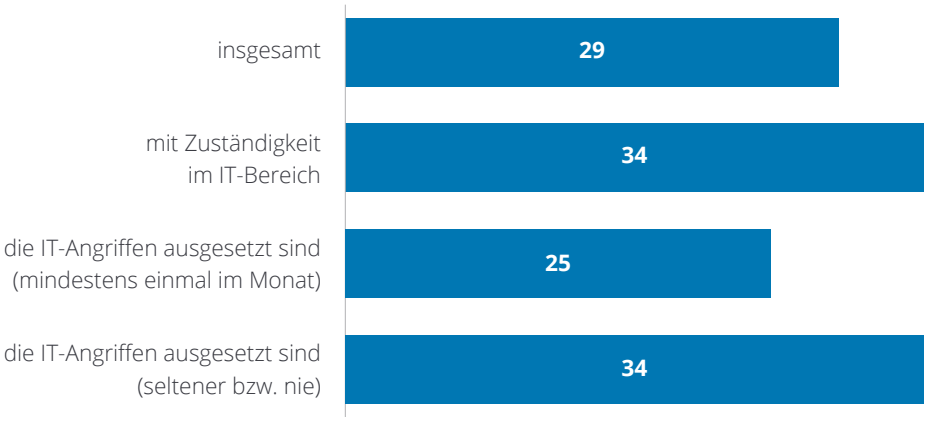
Die wahrgenommene Häufigkeit der Angriffe ist seit Beginn der Trendstudie im Jahr 2013 deutlich gestiegen und verharrt aktuell auf einem hohen Niveau, auch wenn im Vergleich zum letzten Jahr der Wert leicht zurückging. Aktuell berichten 25 Prozent der Führungskräfte von täglichen Angriffen auf das eigene Unternehmen, während es im Vorjahr noch 27 Prozent waren. Allerdings stieg gleichzeitig der Anteil derer, die behaupten, dass ihr Unternehmen nie oder nur selten angegriffen worden ist, von 40 auf 47 Prozent.

Zwar sagt fast die Hälfte der Befragten, ihr Unternehmen werde selten oder nie angegriffen, jedoch räumt auch knapp ein Drittel der Führungskräfte aus großen und mittleren Unternehmen ein, dass Cyber-Angriffe häufig unbemerkt bleiben. Führungskräfte mit Verantwortung im IT-Bereich gestehen dies zu 34 Prozent ein.

Knapp die Hälfte der befragten Führungskräfte ist der Annahme, nie oder nur selten Ziel eines Cyber-Angriffs zu sein, und knapp ein Drittel geht davon aus, dass Angriffe auf ihr Unternehmen unbemerkt bleiben.

Abb. 2 – Cyber-Angriffe bleiben häufig unbemerkt

Mehr als jede vierte Führungskraft geht davon aus, dass Cyber-Angriffe auf das eigene Unternehmen häufig unbemerkt bleiben.

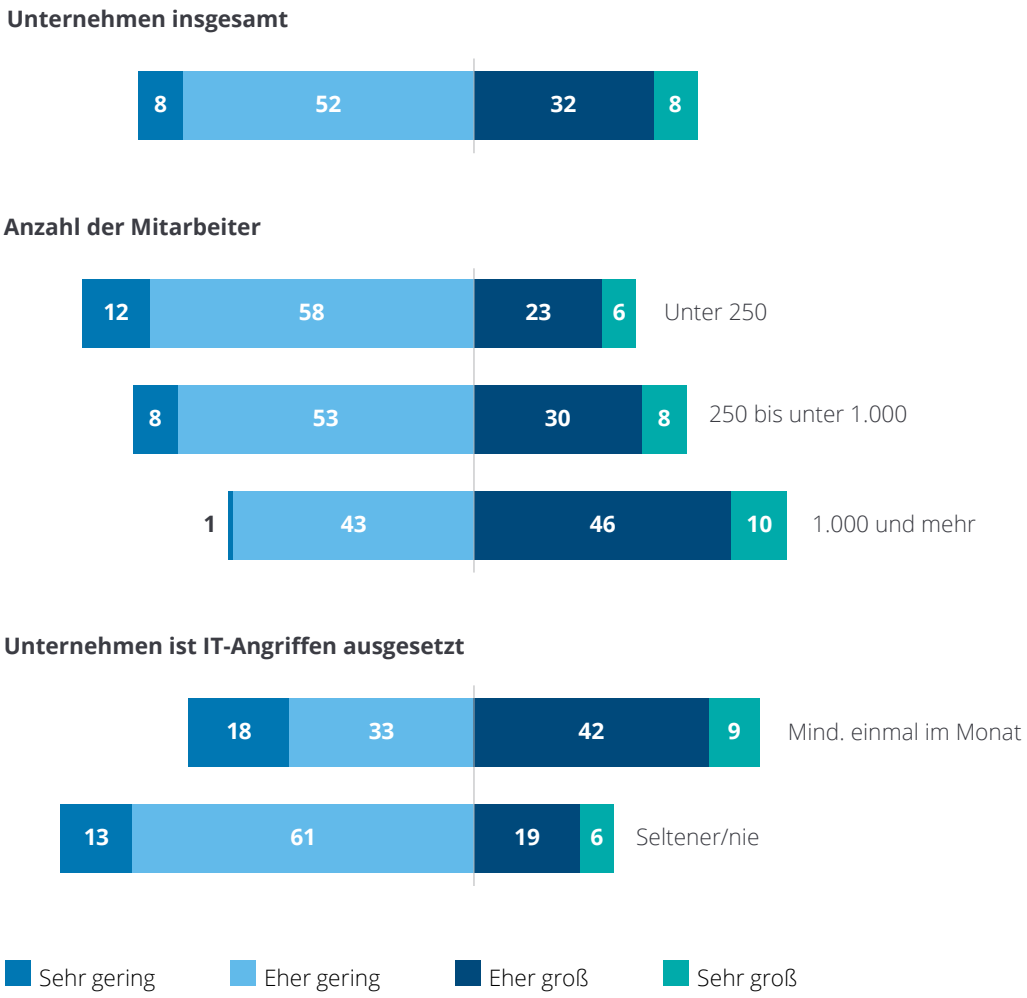


Angaben in Prozent.

Die Einschätzung des Schadensrisikos steigt grundsätzlich mit Unternehmensgröße und Zahl der Angriffe. Während in Unternehmen mit weniger als 250 Mitarbeitern 29 Prozent das Schadensrisiko als groß oder sehr groß bewerten, steigt dieser Wert bei Unternehmen mit mehr als 1000 Mitarbeitern auf 56 Prozent an. Unternehmen, die monatlich oder häufiger angegriffen werden, sind sich der Gefahr anscheinend bewusster und schätzen das Risiko höher ein als diejenigen, die weniger angegriffen werden.

Abb. 3 – Einschätzung des Schadensrisikos steigt mit Unternehmensgröße bzw. Zahl der Angriffe

Nur 40 Prozent der Unternehmen stufen das Risiko einer gravierenden Schädigung durch einen Hackerangriff als (eher) groß ein.



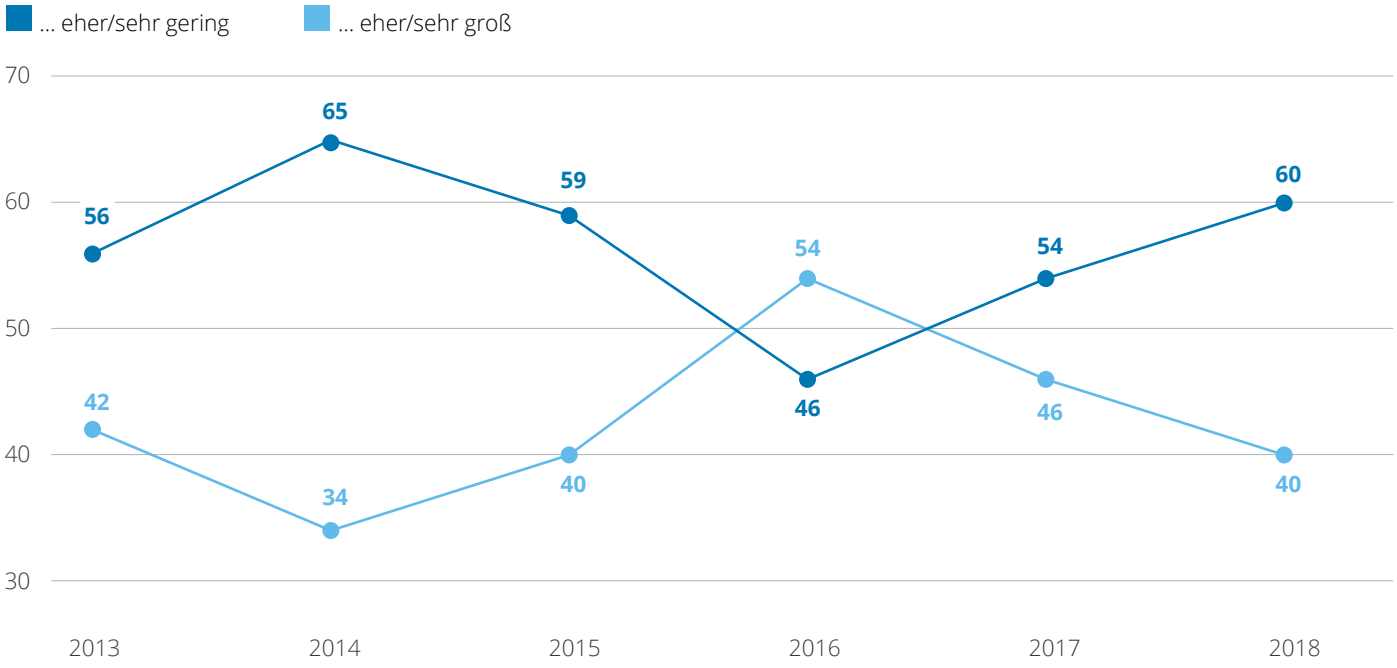
Angaben in Prozent.
Auf 100 fehlende Prozent ergeben sich durch abgerundete Einzelwerte.

Gleichzeitig steigt seit 2016 die Anzahl derer, die das Risiko als eher gering oder sehr gering einschätzen, aktuell sind es 60 Prozent der Befragten. Die Unternehmen vertrauen auf ihre Vorsorgemaßnahmen. Diejenigen, die nach eigener Ansicht so gut wie möglich vorbereitet sind, schätzen das Risiko einer gravierenden Schädigung noch etwas geringer ein.

60 Prozent der Wirtschaftsführer halten den Schaden durch einen Hackerangriff für gering oder sehr gering.

Abb. 4 – Subjektive Einschätzung des Schadensrisikos durch Hackerangriffe im Rückgang

Führungskräfte halten das Risiko, dass ihr Unternehmen durch einen Hackerangriff gravierend geschädigt wird, für ...



Angaben in Prozent.

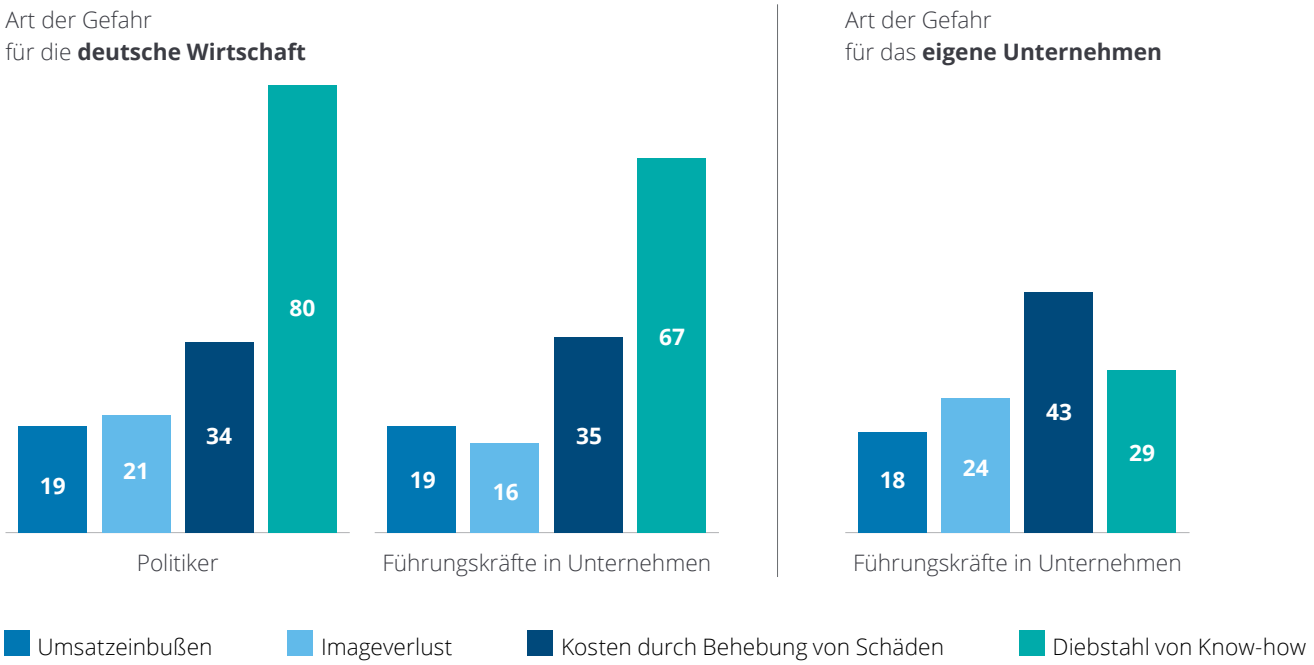
2. Differenzierte Sicht auf die potenziellen Schäden

Laut einer Studie des Branchenverbandes Bitkom[2] sind deutschen Unternehmen in den letzten zwei Jahren Schäden in Höhe von 43,4 Milliarden Euro entstanden. Sabotage, Datendiebstahl oder Spionage waren Gründe dafür.

Die Bewertung möglicher Schäden durch Cyber-Angriffe wird durch die befragten Politiker und Führungskräfte aus der Wirtschaft differenziert gesehen. Als größtes Risiko für die deutsche Wirtschaft sehen Abgeordnete mit 80 Prozent und Führungskräfte mit 67 Prozent den Diebstahl von Know-how. Jeweils rund ein Drittel nennt die Kosten, die durch die Behebung von Schäden entstehen, jeweils rund jeder Fünfte nennt Imageverluste beziehungsweise Umsatzeinbußen.

Für das eigene Unternehmen sehen Führungskräfte das anders. Am häufigsten halten sie die Kosten, die durch die Behebung von Schäden entstehen, für die größte Gefahr, die für ihr Unternehmen von Cyber-Angriffen ausgeht – 43 Prozent. Erst mit deutlichem Abstand folgen Nennungen wie Diebstahl von Know-how, Imageverluste und Umsatzeinbußen.

Abb. 5 – Diebstahl von Know-how – für die Gesamtwirtschaft eher ein Problem als für das einzelne Unternehmen



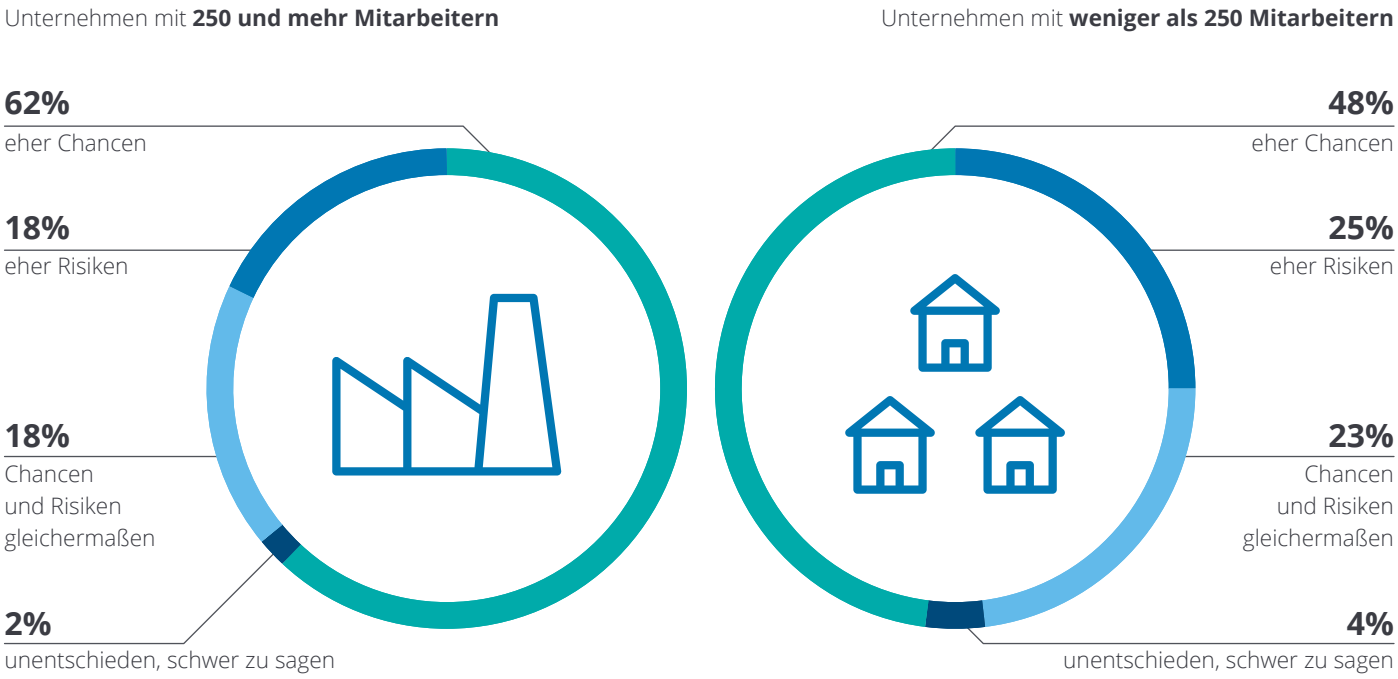
Angaben in Prozent.

[2] Bitkom (2018): Wirtschaftsschutzstudie 2018.

Für ihr eigenes Unternehmen sehen Führungskräfte auch Schäden durch Imageverluste als ein Risiko bei Cyber-Angriffen. Fast ein Viertel der Befragten nimmt hier eine Gefahr wahr. Andererseits sieht aber auch eine knappe Mehrheit Chancen in sozialen Netzwerken, bei den größeren Unternehmen steigt diese Sicht sogar auf über 60 Prozent an.

Know-how-Verlust wird als größte durch Cyber-Angriffe ausgehende Gefahr für die deutsche Wirtschaft gesehen – für das eigene Unternehmen fürchtet man eher die Kosten für das Beheben von Schäden und den Imageverlust.

Abb. 6 – Soziale Netzwerke – für Unternehmen eher Chance als Risiko

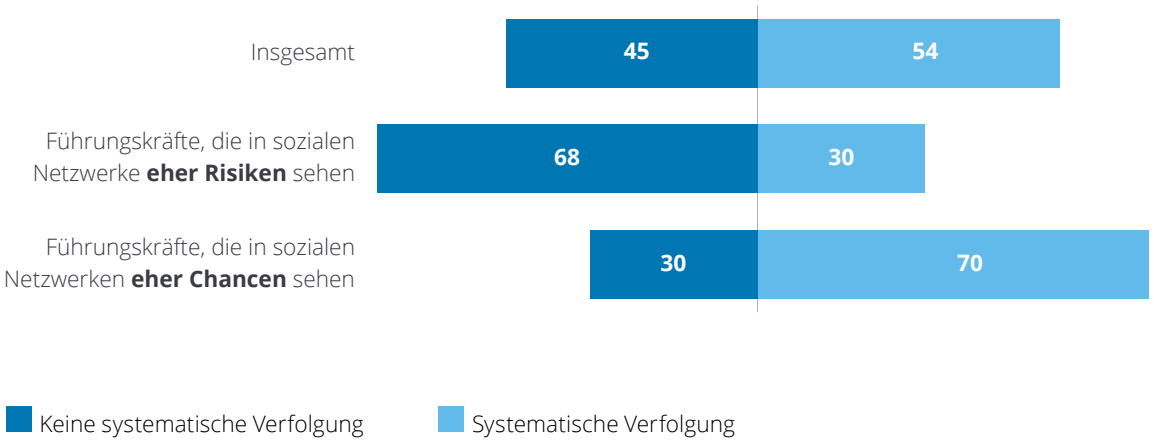


Angaben in Prozent.

Erstaunlich ist, dass viele Unternehmen das Echo in sozialen Netzwerken nicht systematisch verfolgen – insbesondere diejenigen, die in ihnen eher Risiken sehen – aktuell sind es 68 Prozent der Befragten. Könnte das möglicherweise ein Ignorieren des Unbekannten sein? Egal, was die Gründe dafür sein mögen, auch wenn ein Unternehmen nicht die Chancen sieht und soziale Netzwerke nicht aktiv nutzt, sollten die Beobachtung und aktives Kommunikationsmanagement Bestandteil des Risikomanagements sein.

68 Prozent der Unternehmen, die in sozialen Netzwerken eher Risiken sehen, verfolgen das Echo in den Netzwerken nicht systematisch.

Abb. 7 – Viele Unternehmen verfolgen das Echo in sozialen Netzwerken nicht systematisch



Angaben in Prozent.
Auf 100 fehlende Prozent: Weiß nicht, keine Angaben.

„Soziale Netzwerke bieten den Unternehmen zahlreiche Chancen. Stärkere Imagebildung, Gewinnung neuer Kunden und auch gezieltes Recruiting gehören dazu. Soziale Netzwerke sollten Unternehmen stets im Auge behalten, sonst verpasst man die Chancen oder übersieht die Risiken. Schnell können sich negative wirtschaftliche Auswirkungen aus der Schädigung der Reputation ergeben. Das Management von Reputationsrisiken gehört damit in jeden Baukasten des unternehmerischen Risikomanagements."

Katrin Rohmann, Government & Public Services Industry Leader

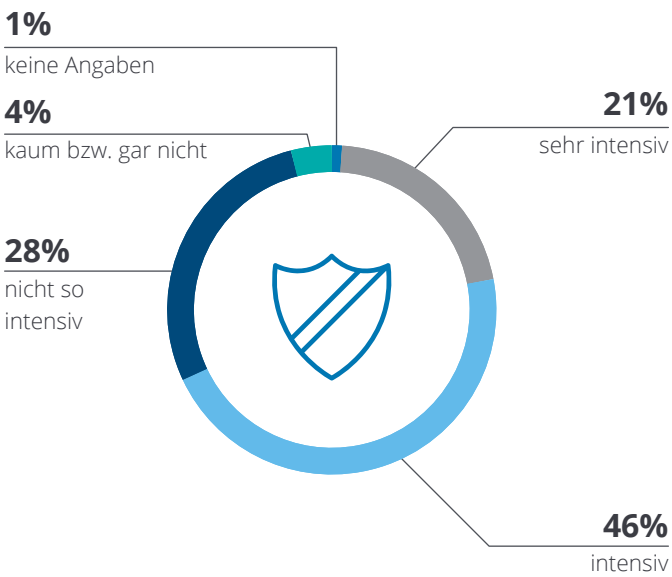
3. Verantwortung und Kompetenz im Unternehmen

Im digitalen Zeitalter ist Cyber-Sicherheit bei einem großen Teil der Unternehmen ein strategisches Thema beziehungsweise eine Aufgabe für die Geschäftsführung. Zwei Drittel der Befragten gaben an, die Geschäftsführung beschäftige sich intensiv oder sehr intensiv und auch regelmäßig damit. Jedoch verbleibt so immer noch ein Drittel, das sich weniger und nur anlassbezogen mit der IT-Sicherheit befasst.

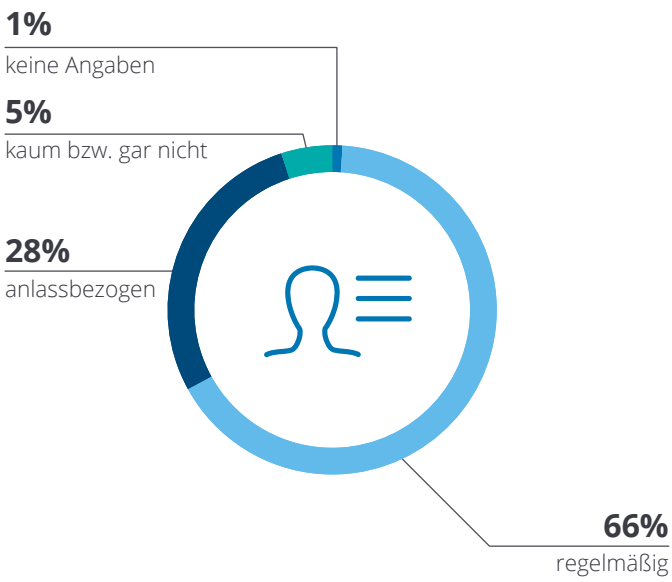
Nach wie vor wird die Kompetenz in den zuständigen Fachabteilungen gesehen, nur eine Minderheit der Befragten sieht in ihrem Unternehmen ausreichend Kompetenz auf Ebene der Geschäftsleitung.

Abb. 8 – Sporadische Befassung mit Cyber-Security durch die Geschäftsführung

Intensität
In rund jedem dritten Unternehmen befasst sich die Geschäftsführung mit dem Thema Cyber Security nicht intensiv, wenn überhaupt ...



Häufigkeit
... und in rund jedem dritten Unternehmen höchstens anlassbezogen.



Rund 50 Prozent der Aufsichtsräte legen Wert auf Informationen über Cyber-Sicherheit.

Schon im letztjährigen Cyber-Security Report haben wir festgestellt, dass in weniger als der Hälfte der befragten Unternehmen mit einem Aufsichtsrat sich dieser auch mit Cyber-Sicherheit befasst. In diesem Jahr haben wir gefragt, ob der Aufsichtsrat Wert auf Informationen zur Cyber-Sicherheit legt. Im Ergebnis trifft dies auch wieder nur knapp für die Hälfte zu.

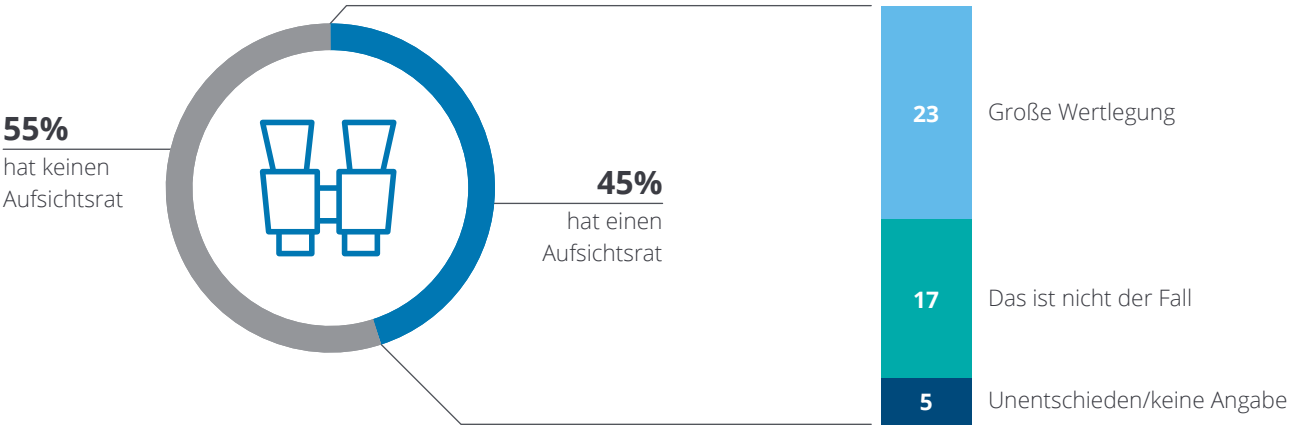
Im Rahmen seiner Rolle bei der regelmäßigen und proaktiven Überwachung der Geschäftsführung ist der Aufsichtsrat auch für den Bereich der Cyber-Sicherheit zur Aufsicht verpflichtet und muss die Schlagkraft der dazu genutzten Maßnahmen bewerten. Das verlangt ein effektives internes Kontroll- und Risikomanagementsystem.

Vor dem Hintergrund der zunehmenden Cyber-Bedrohungen und der potenziellen Auswirkungen auf ein Unternehmen gehören Cyber-Risiken auch zu den strategischen Gefährdungen, die auf die Agenda des Aufsichtsrates gehören.

Abb. 9 – Aufsichtsräte und regelmäßige Informationen zur Cyber-Sicherheit

Das Unternehmen ...

Legt der Aufsichtsrat Wert auf Informationen zur Cyber-Sicherheit?



Angaben in Prozent.

4. Schutz des Unternehmens

4.1 Kosten

In den letzten Jahren haben sich die Cyber-Angriffe auf Unternehmen, auch in Deutschland, stetig vermehrt. Die Intentionen der Angreifer reichen von Spionage über Patentdiebstahl bis hin zu Sabotage. So wurde beispielsweise bewusst das Telekommunikationsnetz eines Energieanbieters im Sommer 2017 angegriffen. Ferner können Unternehmen auch durch Angriffe in Mitleidenschaft gezogen werden, obwohl das Ziel ein ganz anderes war. Das beste Beispiel hierfür war die Malware NotPetya, die unter anderem in einer Art Kettenreaktion mehreren großen deutschen Unternehmen Schaden in Millionenhöhe zufügte.

Schäden werden nicht nur durch den Angriff selbst, sondern zu einem großen Teil durch die Folgekosten verursacht. Durch Datenverluste entstehen außerdem nicht nur Schäden bei einem selbst, sondern auch bei Dritten. Weiterhin gehören zur Wiederherstellung der Geschäftstätigkeit Kosten:

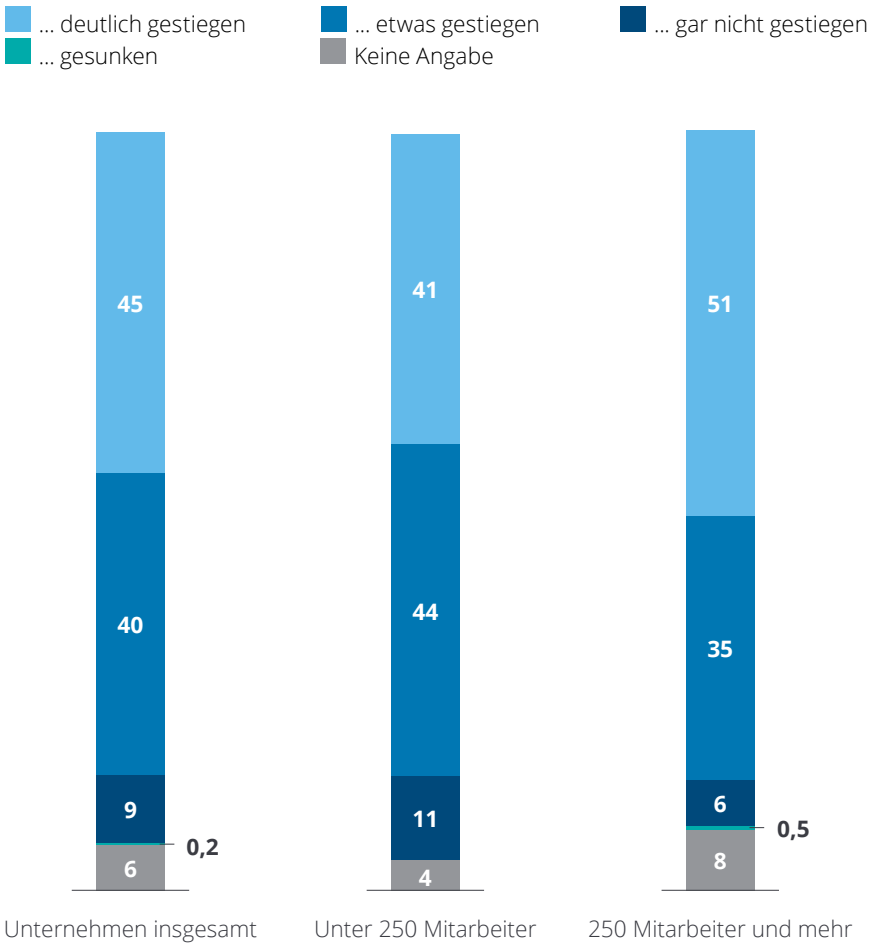
- Für die Wiederherstellung und die Instandsetzung der IT-Systeme
- Zur Fortführung beziehungsweise Wiederaufnahme des Geschäftsbetriebs
- Für die Beauftragung externer IT-Forensiker
- Für Krisenmanagement und Öffentlichkeitsarbeit
- Für Kreditschutz- und Kreditüberwachungsservices
- Für die Beauftragung spezialisierter Anwälte und gegebenenfalls die strafrechtliche Verteidigung

Vor diesem Hintergrund ist es nicht überraschend, dass die Kosten für IT-Sicherheit in den letzten zwei bis drei Jahren nach den Angaben einer überwiegenden Mehrheit der Führungskräfte gestiegen sind. Dabei geben 45 Prozent zu Protokoll, die Kosten seien deutlich gestiegen, und 40 Prozent berichten von einer leichten Kostensteigerung in diesem Bereich. Von gesunkenen Kosten für IT-Sicherheit berichtet praktisch keiner der Befragten.

85 Prozent der Unternehmen berichten von gestiegenen Kosten in der IT-Sicherheit.

Abb. 10 – Entwicklung der Kosten für die IT-Sicherheit

Die Kosten für die IT-Sicherheit gegen Hackerangriffe sind ...



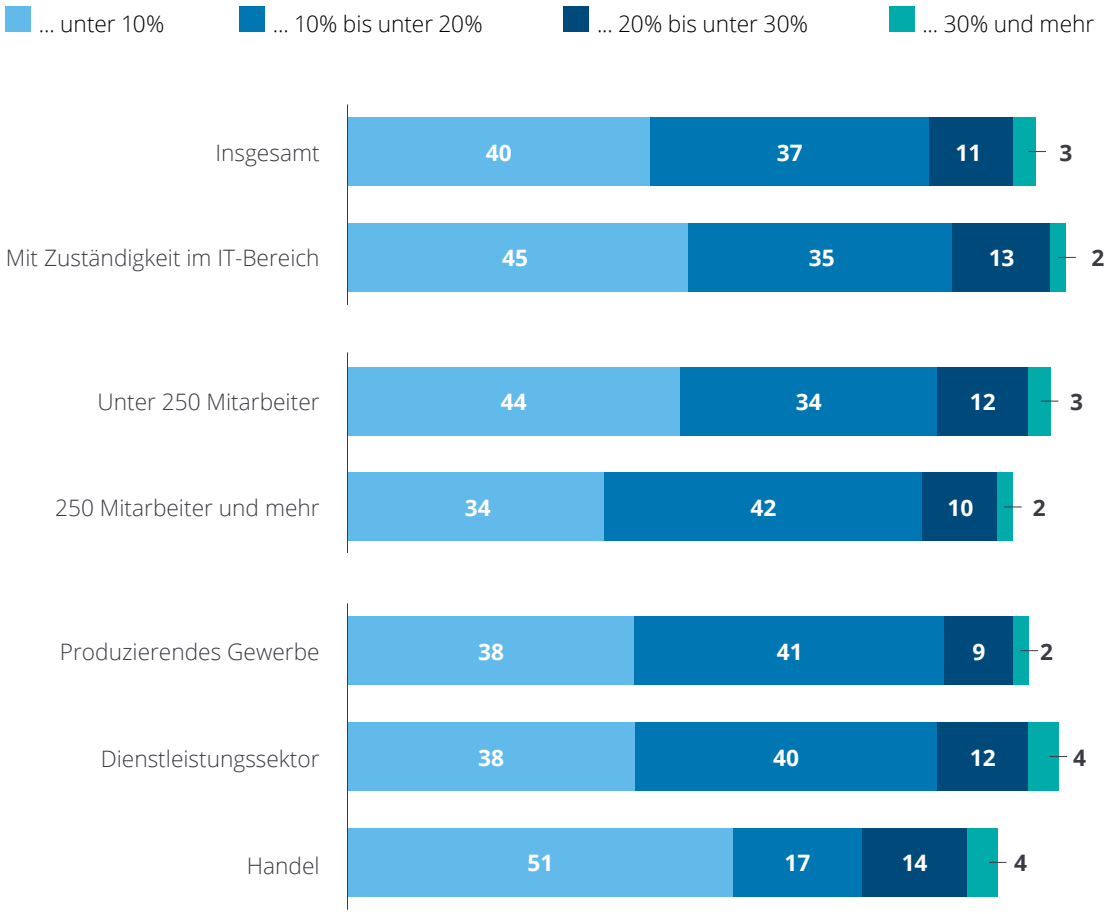
Angaben in Prozent.

„Proaktives Anpassen von Cyber-Security-Maßnahmen kann einem Unternehmen Ressourcen einsparen und ihm helfen vor die Lage zu kommen. Führungskräfte können sich auch stets das aktuellste Know-how ins Unternehmen holen, wenn sie Teile oder auch komplette Cyber-Security-Prozesse auslagern. So können sie sich auf ihr Kerngeschäft konzentrieren."

Peter Wirnsperger, Cyber Risk Leader

Abb. 11 – Häufig wird noch nicht einmal jeder zehnte Euro im IT-Bereich für Sicherheit ausgegeben

Führungskräfte schätzen den Anteil der Kosten für IT-Sicherheit an den Gesamtkosten für IT in ihrem Unternehmen auf ...



Angaben in Prozent.
Auf 100 fehlende Prozent: Weiß nicht, keine Angaben.

Überdurchschnittlich hoch ist der Anteil der sicherheitsbezogenen IT-Ausgaben in größeren Unternehmen ab 250 Mitarbeitern. In Handelsunternehmen geben dagegen 51 Prozent der Unternehmen im Bereich IT weniger als jeden zehnten Euro für Sicherheit aus.

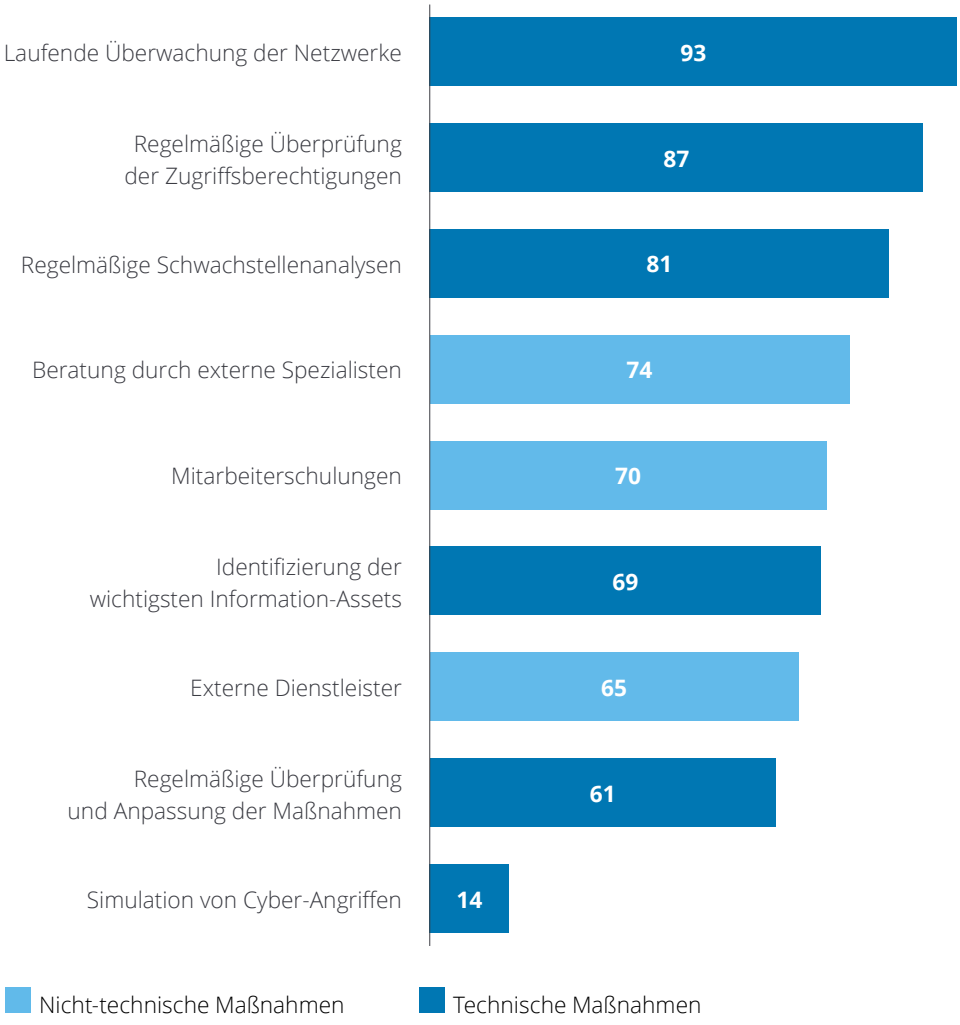
Vor dem Hintergrund der zunehmenden Cyber-Angriffe, der immer neueren Cyber-Waffen und der ansteigenden Ausgaben der Unternehmen für IT-Sicherheit ist es aber erstaunlich, dass – gemessen an den Gesamtausgaben für den IT-Bereich – die Kosten für IT-Sicherheit bei der großen Mehrheit der Unternehmen bei weniger als einem Fünftel liegt. 40 Prozent der befragten Unternehmen investieren nach Auskunft ihrer Führungskräfte sogar weniger als zehn Prozent der IT-Gesamtausgaben in Sicherheit. Die Schätzungen der Verantwortlichen, die in ihrem Unternehmen für den IT-Bereich zuständig sind, weichen von den Schätzungen der Führungskräfte insgesamt nur wenig ab, liegen tendenziell aber eher darunter.

4.2 Maßnahmen

Zum Schutz ihrer IT-Infrastruktur ergreifen viele Unternehmen zwar eine Reihe von Maßnahmen, aber nur ein kleiner Teil schöpft die Möglichkeiten aus, die eigene Sicherheit im IT-Bereich zu optimieren. So überwachen fast alle Unternehmen ihre IT-Netzwerke laufend, 87 Prozent überprüfen die Zugriffsrechte ihrer Mitarbeiter regelmäßig, das heißt mindestens einmal im Jahr, 81 Prozent führen regelmäßig Schwachstellenanalysen ihrer Netzwerke und wichtigsten Geschäftsanwendungen durch.

Abb. 12 – Maßnahmen zum Schutz der IT-Infrastruktur

Folgende Maßnahmen werden zum Schutz der IT-Infrastruktur ergriffen:



Angaben in Prozent/Mehrfachnennungen möglich.

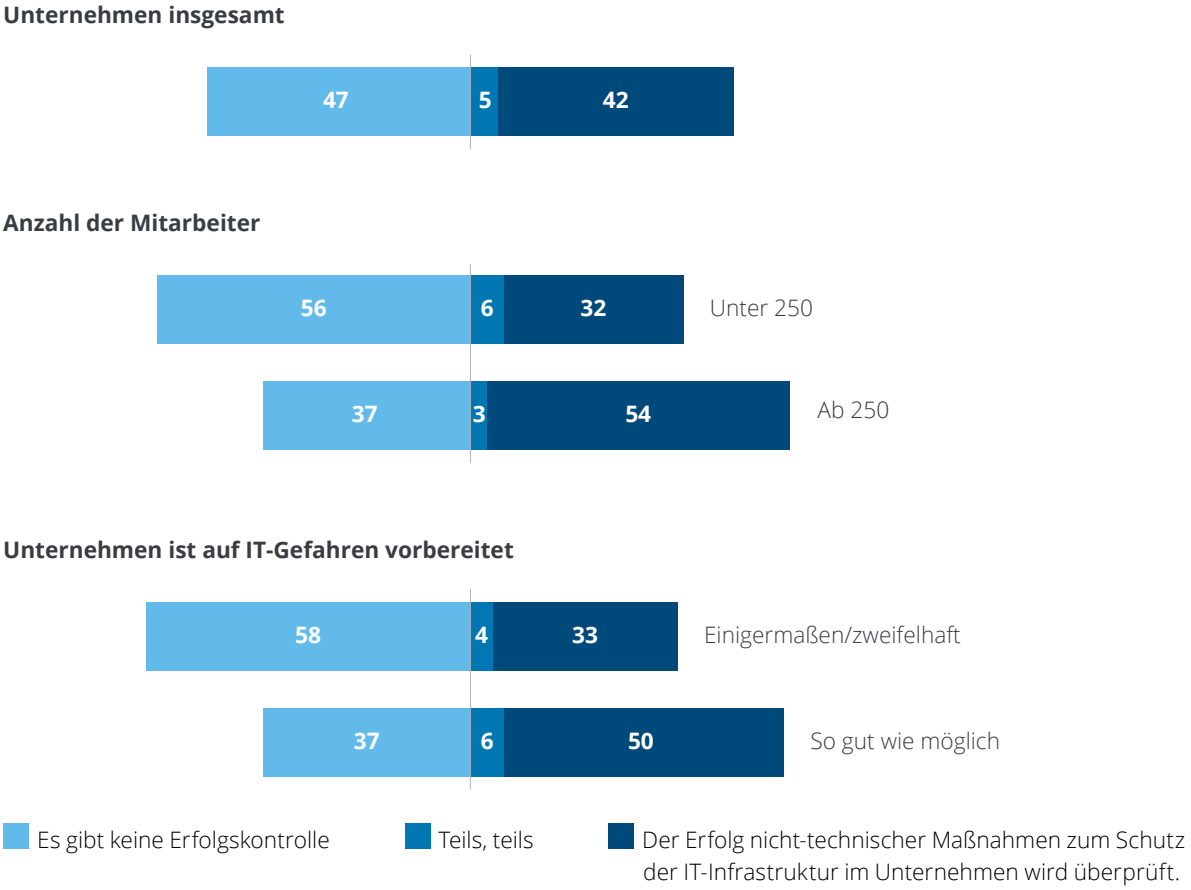
Eine Identifizierung der wichtigsten Information-Assets, die von Cyber-Angriffen betroffen sein könnten, haben dagegen lediglich rund zwei Drittel der Unternehmen vorgenommen, nur 61 Prozent überprüfen regelmäßig, ob die zum Schutz der wichtigsten Assets getroffenen Maßnahmen ausreichen, und passen diese Vorkehrungen gegebenenfalls an. Planspiele zur Simulation von Cyber-Angriffen, beispielsweise War Gaming oder Red Teaming, führen gerade einmal 14 Prozent der Unternehmen regelmäßig durch. Von den sechs genannten möglichen Maßnahmen zur Erhöhung der Cyber-Sicherheit ergreift rund ein Drittel der Unternehmen nur drei oder weniger.

Auch andere, nicht-technische Maßnahmen zur Verbesserung der IT-Sicherheit werden zwar von vielen Unternehmen ergriffen, die Möglichkeiten, die IT-Sicherheit zu erhöhen, aber auch in diesem Feld häufig nicht ausgeschöpft. So suchen 74 Prozent der Unternehmen bei externen Spezialisten Rat, welche aktuellen Entwicklungen es im Bereich Cyber-Security gibt und wie man sich am besten darauf einstellen kann. Dem möglichen Einwand, dass dies ja auch nur nötig sei, wenn die eigene IT-Abteilung nicht ausreichend kompetent ist, steht entgegen, dass sehr große Unternehmen mit 1.000 und mehr Mitarbeitern tendenziell überdurchschnittlich häufig auch auf externen Rat setzen.

70 Prozent der Unternehmen führen regelmäßig, das heißt mindestens einmal jährlich, Schulungen für ihre Mitarbeiter im Bereich IT-Sicherheit durch. 65 Prozent haben externe Dienstleister beauftragt, die sich um das Thema Cyber Security in ihrem Unternehmen kümmern. Diese Option nutzen Unternehmen ab 1.000 Mitarbeitern nur unterdurchschnittlich häufig. Rund jedes vierte Unternehmen beziehungsweise jedes fünfte Unternehmen ab 1.000 Mitarbeitern nutzt nur eine oder gar keine der drei genannten nicht-technischen Möglichkeiten zur Erhöhung der IT-Sicherheit – das sagen aktuell 24 Prozent beziehungsweise 21 Prozent.

Ob die genannten nicht-technischen Maßnahmen wie Beratung durch externe Spezialisten, Mitarbeiterschulungen oder externe Dienstleister wirklich zur Verbesserung der IT-Sicherheit beitragen, wird nur von 42 Prozent der Unternehmen kontrolliert, die mindestens eine der drei durchführen, weitere 5 Prozent überprüfen das bei manchen der Maßnahmen. Rund die Hälfte dieser Unternehmen und 37 Prozent der Unternehmen ab 1.000 Mitarbeitern führen keinerlei Erfolgskontrollen bei diesen Maßnahmen durch. Noch am häufigsten wird offenbar der Erfolg von Mitarbeiterschulungen überprüft, am wenigsten häufig der Beitrag externer Dienstleister zur Verbesserung der IT-Sicherheit des Unternehmens.

Abb. 13 – Erfolgskontrollen nicht-technischer Maßnahmen finden nur teilweise statt



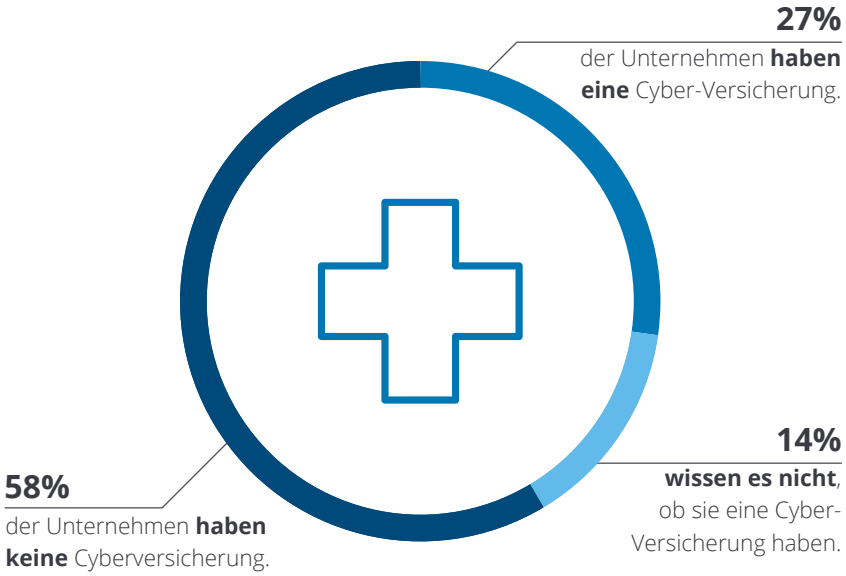
Angaben in Prozent.
Über 100 Prozent ergeben sich durch aufgerundete Einzelwerte.

„Ein Unternehmen kann sich technisch nicht perfekt absichern. Deswegen gehören Maßnahmen zur Erhöhung der organisatorischen Resilienz wie War Gaming und Red Teaming zum Üben des Ernstfalls dazu. Sie überprüfen und verbessern die Wirksamkeit von Schutzmaßnahmen, Prozessen und Handlungsweisen."

Peter J. Wirnsperger, Cyber Risk Leader

Abb. 14 – Die meisten Unternehmen haben keine Cyber-Versicherung

Nur **rund ein Viertel** der Führungskräfte kann bestätigen,
dass das eigene Unternehmen eine solche Versicherung abgeschlossen hat.



Nur Unternehmen, die eine konkrete Angabe gemacht haben.
Auf 100 fehlende Prozent ergeben sich durch gerundete Werte.

Nach der Vermeidung und Abwehr von Risiken, der Minimierung und dem Umgang mit dem eingetretenen Fall ist auch eine Versicherung ein klassisches Mittel des Risikomanagements. So existieren seit einiger Zeit auch sogenannte Cyber-Versicherungen. Hierbei handelt es sich meist um eine Verknüpfung aus Haftpflicht-, Betriebsausfall- und Datenversicherung für Dritt- (z.B. Datenrechtsverluste) und Eigenschäden in Form von Vermögensschäden, gegebenenfalls ergänzt um eine Betriebsunterbrechungsversicherung. Hierbei handelt es nicht nur um die direkten Schäden des Angriffs, sondern auch um die Kosten für die Wiederherstellung des Geschäftsbetriebs.

Jedoch geben trotz der hohen Bewertung von Kosten als größten Schaden durch Cyber-Angriffe und der bei vielen herrschenden Meinung, nicht bestmöglich vorbereitet zu sein, 58 Prozent der befragten Führungskräfte an, sie seien nicht durch eine Cyber-Versicherung abgesichert. 14 Prozent wissen es sogar nicht.

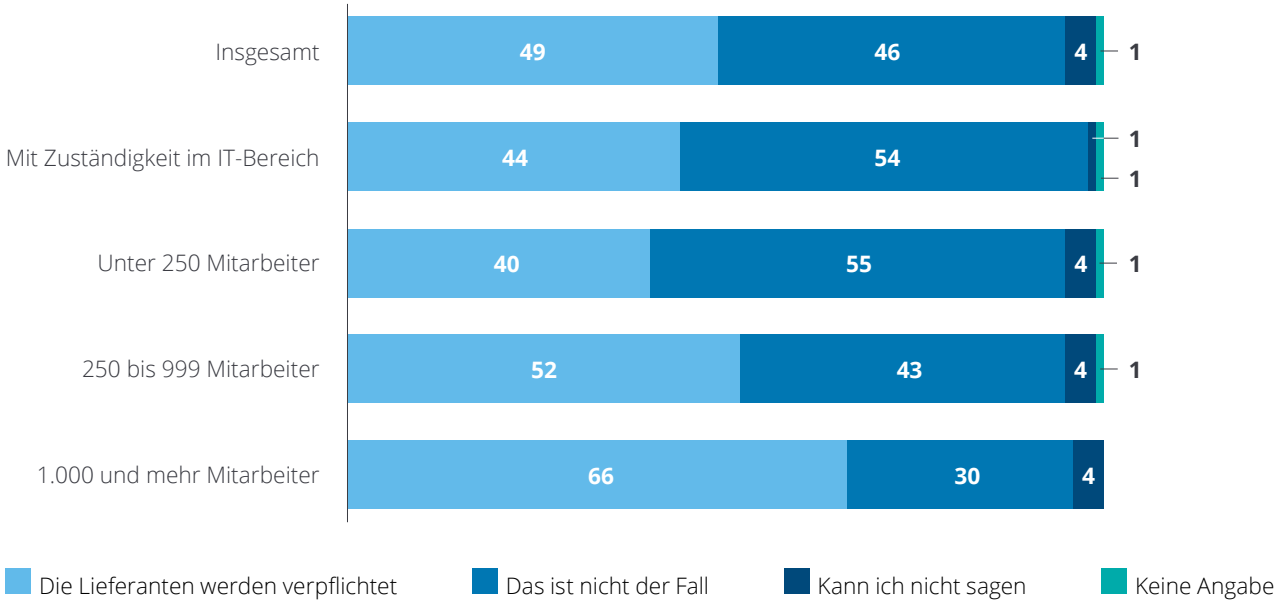
4.3 Sicherheit erfordert Kooperation

Da Cyber-Angriffe oftmals Kettenreaktionen auslösen können und sehr schwer greifbar und einzugrenzen sind, machen Risiken aus dem Cyber-Raum nicht an der Unternehmensgrenze halt. Daher sind Unternehmen auch grundlegend verpflichtet, in ihren Lieferketten auf Cyber-Risiken einzugehen und beispielsweise Lieferanten in die Pflicht zu nehmen, bestimmte IT-Sicherheitsstandards einzuhalten. Vor diesem Hintergrund ist es jedoch interessant zu sehen, dass nur rund jedes zweite Unternehmen seine Lieferanten verpflichtet, IT-Sicherheitsstandards einzuhalten. Hier zeigt sich, dass ein erhöhtes Bewusstsein diesbezüglich bei den Unternehmen noch notwendig ist.

Nur rund jedes zweite Unternehmen verpflichtet seine Lieferanten auf die Einhaltung von IT-Sicherheitsstandards.

Abb. 15 – Verpflichtung von Lieferanten auf die Einhaltung von IT-Sicherheitsstandards

Verpflichten Sie Ihre Lieferanten zur Einhaltung bestimmter IT-Sicherheitsstandards, oder ist das nicht der Fall?



Angaben in Prozent.

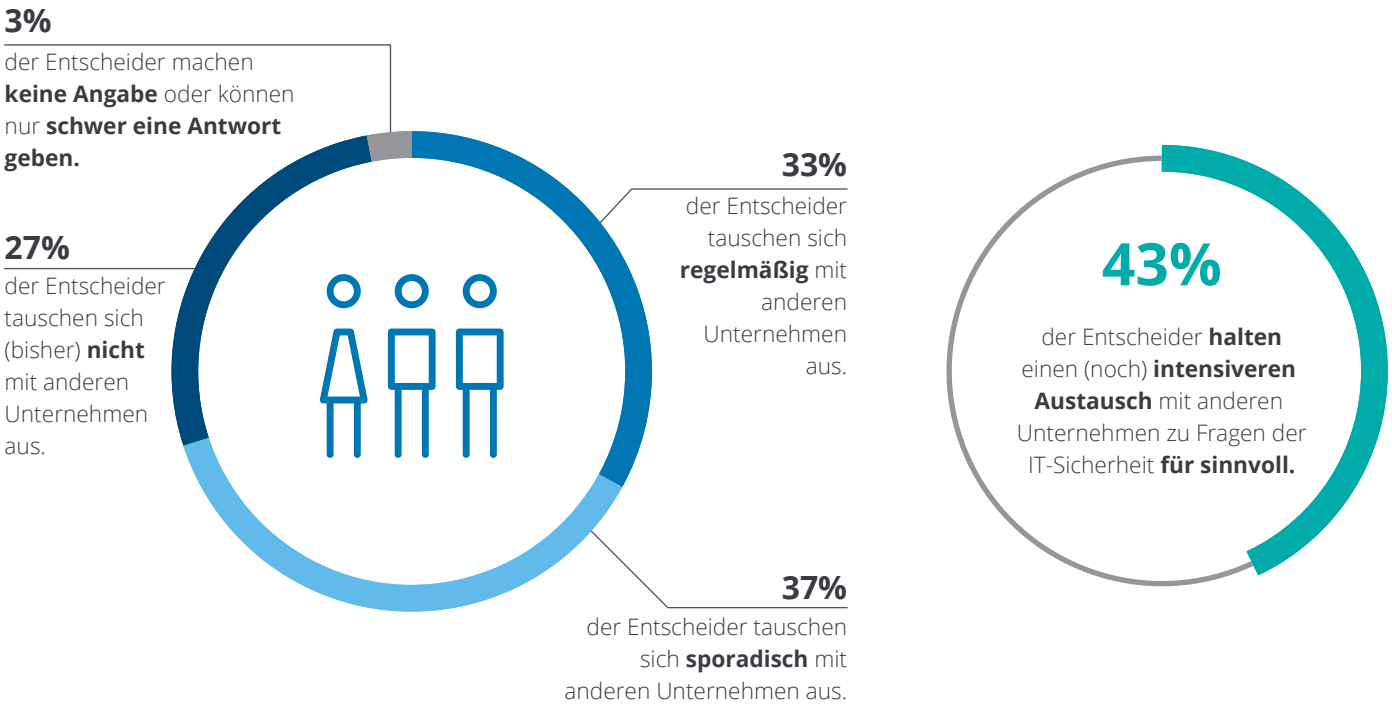
Austauschformate wie die Allianz für Cyber-Sicherheit, die den Austausch zwischen Unternehmen (seien es IT-Dienstleistungs- und -Beratungsunternehmen oder IT-Hersteller) und (staatlichen) Institutionen fördert, dienen dazu, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken. Bei der Cyber-Sicherheit wird auch oft betont, dass ein Informationsaustausch über Erfahrungen mit Angriffen oder über Best Practices in Bezug auf die Resilienz und Verteidigung sehr wichtig ist. Vor diesem Hintergrund ist es überraschend, dass eine Mehrheit der Unternehmen einen Austausch mit anderen Unternehmen zu Fragen der IT-Sicherheit für nicht sinnvoll erachtet. Einen regelmäßigen Austausch sehen sogar weniger als ein Drittel als wirksam an.

Viele Unternehmen arbeiten beispielsweise heute schon bei sogenannten Threat-Intelligence-Plattformen und bei der Speicherung und Verwertung von Gefährdungsindikatoren mehr oder weniger intensiv zusammen.

Die gemeinsame Nutzung kann eine große Hilfe zur schnellen und effektiven Erkennung von Angriffen sein: Oftmals werden ähnliche Organisationen von demselben Bedrohungsakteur gleichzeitig oder auch zeitversetzt angegriffen. Threat-Intelligence-Plattformen (TIP) helfen, diesen Bedrohungen zu begegnen. Das Teilen von Informationen ermöglicht eine gemeinsame Analyse und verhindert die Gefahr von Doppelarbeiten.

Das Hauptziel ist es hierbei, sich zu allseitigem Vorteil Informationen über Taktiken, Techniken und Verfahren von Angreifern auszutauschen und sich über adäquate Reaktionen zu informieren. TIP bieten die Möglichkeit, Indicators of Compromise (IOC) und Informationen über Malware strukturiert zu speichern und Korrelationen, automatisierte Exporte für Intrusion-Detection-Systeme oder das Security-Information- und Event-Management durchzuführen. So können nützliche Daten ohne Aufwand und automatisiert genutzt werden.

Abb. 16 – Wunsch nach intensiverem Austausch über IT-Sicherheit



„Der Austausch und die gemeinsame Nutzung von Bedrohungsinformationen stehen erst am Anfang. Es gibt gute Initiativen und etablierte Plattformen, die es Unternehmen ermöglichen, durch einen Informationsvorsprung widerstandsfähiger gegenüber Cyber-Angriffen zu werden."

Katrin Rohmann, Government & Public Services Industry Leader

Handlungsfelder

Risikobewusstsein schärfen
Führungskräfte stufen das Risiko, durch einen Hackerangriff geschädigt zu werden, mehrheitlich gering ein – obwohl sie gleichzeitig vermehrt Cyber-Angriffe wahrnehmen. Simulationen wie War Games und Red Teaming können helfen, das Risikobewusstsein auf Führungsebene zu schärfen.

Verantwortung übernehmen
Noch nicht in allen deutschen Unternehmen ist das Thema Cyber-Sicherheit genügend professionalisiert. Die Steuerung von Cyber-Risiken ist eng verbunden mit der Strategieentwicklung von Unternehmen und liegt damit in der Verantwortung von Geschäftsführung und Aufsichtsrat.

Chance versus Risiko in sozialen Netzwerken
Unternehmen sehen die Chancen, die in der Nutzung sozialer Netzwerke liegen. Sie sehen aber auch die Gefährdung durch Fake News und fürchten Reputationsschäden. Die Beobachtung von sozialen Netzwerken und aktives Kommunikationsmanagement müssen Bestandteil des Risikomanagements werden.

Kooperationen sichern
Mit der Digitalisierung der Geschäftsprozesse gewinnt der Aspekt „Sicherheit" immer mehr an Bedeutung. Cyber-Sicherheit sollte nicht nur die interne Wertschöpfung, sondern auch Maßnahmen innerhalb der gesamte Wertschöpfungskette von Anfang bis Ende zuverlässig berücksichtigen.

Resilienz von Organisationen stärken
Ein perfekter Schutz gegen Cyber-Bedrohungen ist trotz steigender Kosten nicht darstellbar. Daher sollten Unternehmen vor allem die Anpassungs- und Widerstandsfähigkeit steigern. Organisatorische Resilienz bietet einen umfassenderen und effizienteren Schutz.

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 12/2018