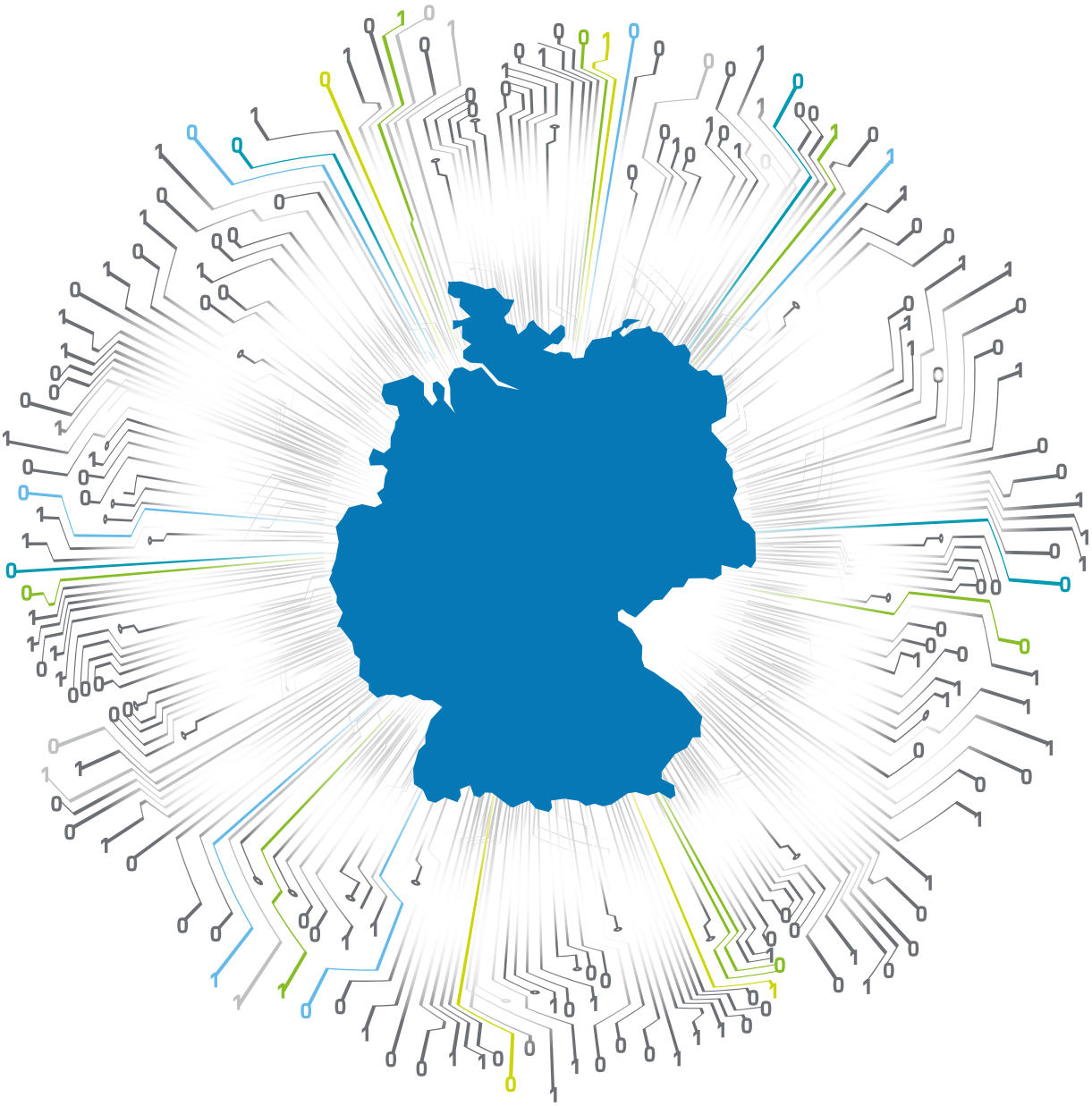
Deloitte.



Cyber Security Report 2019

Teil 2: Die Gefährdung steigt – hält die Sicherheit Schritt?

Vorwort

Der rasant voranschreitende technologische Wandel und die verbindende Kraft der Digitalisierung bringen eine Welle innovativer Produkte und Dienstleistungen hervor. Sie verändern die Lebens- und Arbeitsweise des 21. Jahrhunderts und schaffen ungeahnte wirtschaftliche Chancen für Unternehmen.

Der technologische Wandel bringt aber auch neue Angriffsvektoren für Kriminelle und existenzbedrohende Risiken mit sich. Unternehmen aller Größen und Branchen sollten auf diese Risiken vorbereitet sein und stets aufs Neue prüfen, was aktuelle Entwicklungen für das eigene Unternehmen bedeuten.

Schwachstellen in der Cyber-Sicherheit sind schon heute überall zu erkennen und werden in Zukunft noch häufiger zu finden sein. Beispiele dafür sind der zunehmende Einzug von Industrial Control Systems (ICS) in der Produktion und das Internet of Things (IoT) in fast jedem anderen Bereich. Clients, Handscanner und andere Komponenten mit Netzwerkanschluss können durch genau diese Verbindung eine Schwachstelle darstellen. Angriffe auf die Informationsinfrastrukturen werden zunehmend komplexer und professioneller.

Cyber-Sicherheit ist ein Teil des umfassenden Risikomanagements. Es ist ein ganzheitlicher Prozess, der die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, Anwendungen und IT-Systemen gewährleistet. Somit sollte Cyber-Sicherheit nicht nur eine Frage der Technik, sondern auch eine Frage der personellen und organisatorischen Rahmenbedingungen sein.

Um ein Unternehmen resilient aufzustellen, ist es essenziell, das entsprechende Know-how an Bord zu holen. Neben dem Wissen rund um die Themen Informationssicherheitsmanagementsysteme, IT-Risikomanagement und Sicherheitsmanagement im Allgemeinen sind auch fundierte Erfahrungen mit gängigen Netzwerken, Systemen, Anwendungsentwicklungen und Rechenzentren vonnöten. Die Nachfrage nach solchen IT-Sicherheitstalenten ist höher als das Angebot und die nachhaltige Rekrutierung kann sogar zum Wettbewerbsvorteil werden.

Vor dem Hintergrund der beschriebenen Zusammenhänge haben wir den vorliegenden zweiten Teil des diesjährigen Cyber Security Report auf folgende Themen fokussiert:

- Resilienz
- Fachkräfte
- Industrie 4.0

In Teil 1 der Studie haben wir auf die 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 des Teils der 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

Gefährdung
Wahrgenommene IT-Angriffe steigen stetig an – insbesondere große Unternehmen haben damit zu tun. 40 Prozent von ihnen werden täglich angegriffen. Mittlerweile berichten auch über 20 Prozent der mittleren und großen Unternehmen von spürbaren oder massiven Schäden.

Verantwortung
Die Bedeutung von Cyber-Sicherheit nimmt deutlich zu. Mehr als zwei Drittel der Befragten sehen das so – in großen Unternehmen fast 90 Prozent. Dies hat primär damit zu tun, dass die IT-Infrastruktur eine immer größere Rolle spielt und es gleichzeitig zu mehr Angriffen kommt. Zwar geben über 70 Prozent an, definierte Prozesse zur Identifikation und Bewertung von Cyber-Risiken zu haben, die Berichtsform ist bei vielen aber wenig formalisiert. In gut einem Drittel der Unternehmen wird die Führungsebene nur anlassbezogen über Cyber-Sicherheit informiert. Ein Großteil verlässt sich bei dem Thema auf Experten.

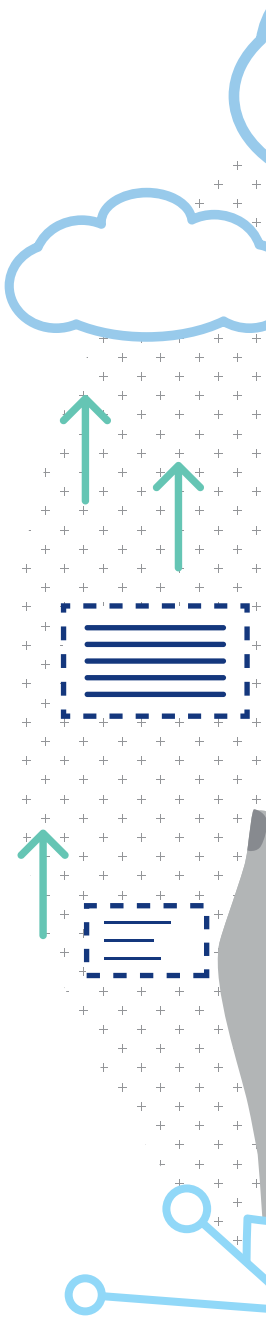
Resilienz und Maßnahmen zum Schutz
Aus Sicht von Sicherheitsverantwortlichen sind verknüpfte Maßnahmen aus Sensibilisierung, Training, technischen Vorkehrungen, Risikomanagement und die Fähigkeit zur wirksamen Reaktion auf laufende Angriffe die beste Kombination, das Risiko durch Cyber-Angriffe zu minimieren.

Cyber-Resilienz wird als erstrebenswerte Qualität angesehen und bietet einen geeigneten Ordnungsrahmen, um die verschiedenen erforderlichen Fähigkeiten in Reaktion auf Cyber-Risiken zu steuern; gleichzeitig ist der Begriff Cyber-Resilienz für viele noch abstrakt und nicht hinreichend definiert.

Die große Mehrheit der Unternehmen setzt auf Schutzstandards wie Überwachung ihrer Netzwerke, Revalidierung von Zugriffsberechtigungen oder Schwachstellenanalysen. Knapp drei Viertel lassen sich dabei von externen Spezialisten beraten und über zwei Drittel haben externe Dienstleister beauftragt, die sich um Cyber-Security kümmern. Insbesondere große Unternehmen verpflichten auch ihre Dienstleister zur Einhaltung bestimmter IT-Sicherheitsstandards.

Fachkräfte
Unternehmen setzen vor allem auf externe Dienstleister und die Fortbildung ihrer Mitarbeiter. Die Rekrutierung von entsprechend qualifizierten Fachkräften auf dem Arbeitsmarkt ist dagegen nur für ein Fünftel ein wesentliches Mittel, um ausreichend Expertise im Bereich IT-Sicherheit im eigenen Unternehmen sicherzustellen. Gut ein Drittel der mittleren und großen Unternehmen berichtet von größeren Schwierigkeiten, ausreichend Fachkräfte für den Bereich IT-Sicherheit zu finden.

Industrie 4.0
Knapp mehr als die Hälfte der Führungskräfte haben sich (sehr) intensiv mit dem Thema Industrie 4.0 auseinandersetzen. Ähnlich sieht es bei Abgeordneten aus, wo 55 Prozent angegeben haben, dass sie sich (sehr) intensiv mit dem Thema auseinandersetzen. Allerdings berichten nur 28 Prozent der Führungskräfte, die sich mit dem Thema Industrie 4.0 näher beschäftigt haben, davon, dass sich die Cyber-Security-Strategie ihres Unternehmens im Zusammenhang mit dem Thema Industrie 4.0 deutlich verändert hat. In Bezug auf Sicherheit der Nutzung des 5G-Standards zur Vernetzung von Produktionsabläufen äußert nur eine Minderheit der Wirtschaftsführer Bedenken.




!
NEWS

1. Einschätzung der Gefährdung

Cyber-Angriffe oder Daten-Leaks gehören mittlerweile zum Alltag. Kaum eine Woche vergeht, ohne dass von den Medien über größere und kleinere Vorfälle berichtet wird. Beispielsweise wird Mitte September innerhalb von zwei Tagen einmal über ein großes Daten-Leak berichtet, bei dem die gesamte Bevölkerung Ecuadors betroffen ist, und zum anderen über einen Fall, bei dem 16 Millionen radiologische Patientendatensätze aus 50 Ländern zugänglich waren.

Unsere Befragung bestätigt, dass diese Gefährdung wahrgenommen wird.

Dazu fragen wir jedes Jahr die Unternehmensvertreter nach der Häufigkeit von IT-Angriffen, die das Unternehmen ausspionieren oder schädigen sollen: So sehen sich fast alle mittleren und großen Unternehmen in Deutschland Cyber-Angriffen ausgesetzt (85 Prozent). Lediglich 4 Prozent der Führungskräfte geben zu Protokoll, ihr Unternehmen sei noch nie angegriffen worden. 11 Prozent können dazu keine Auskunft geben. 28 Prozent der Unternehmen berichten von täglichen Angriffen, bei weiteren 19 Prozent kommt das mindestens einmal wöchentlich vor. Besonders häufig haben große Unternehmen mit Cyber-Attacken zu tun: Unternehmen mit 1.000 und mehr Mitarbeitern zu 40 Prozent täglich.

Abb. 1 – Deutsche Unternehmen als Ziel von IT-Angriffen
Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt, durch die Ihr Unternehmen ausspioniert oder geschädigt werden soll?

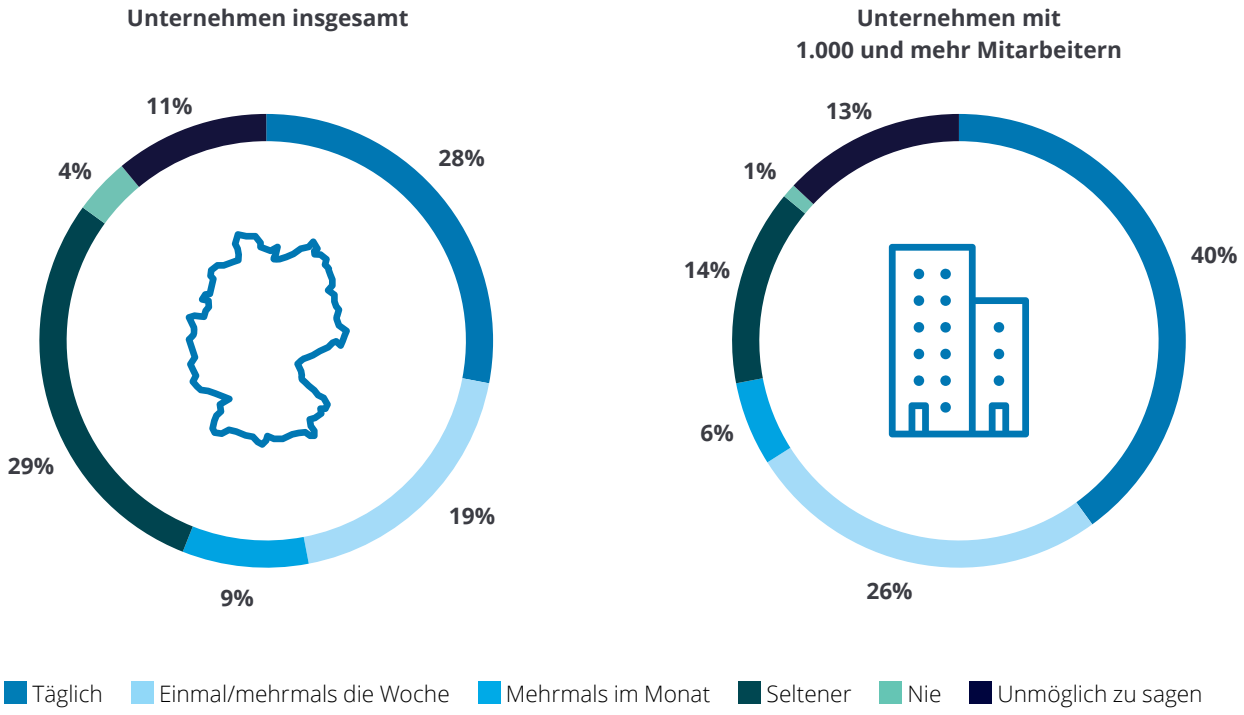
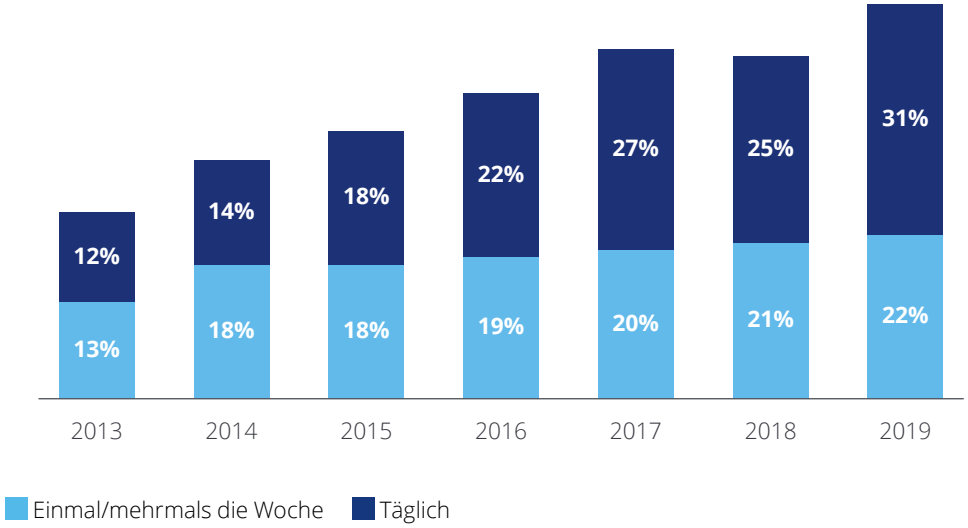


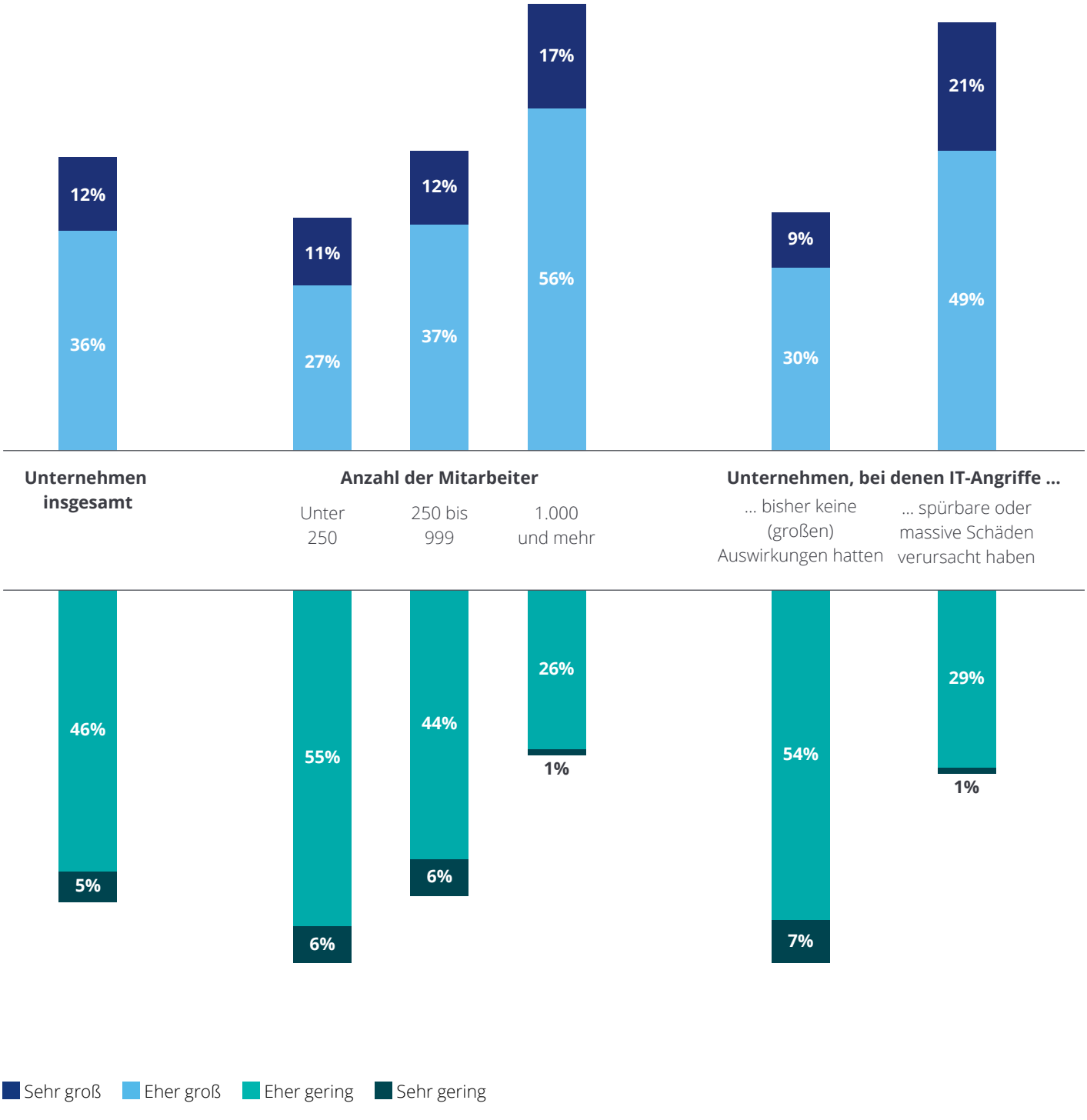
Abb. 2 – Wahrgenommene Häufigkeit von IT-Angriffen wieder gestiegen
Wie häufig ist Ihr Unternehmen IT-Angriffen ausgesetzt, durch die Ihr Unternehmen ausspioniert oder geschädigt werden soll? Nur Unternehmen, die eine konkrete Angabe gemacht haben.



Die Frequenz der Angriffe hat dabei im Vergleich zu den Vorjahren weiter zugenommen und der Anteil derer, die sagen, sie würden einmal die Woche bis täglich angegriffen, liegt sogar sieben Prozentpunkte höher als im vergangenen Jahr.

Bei rund einem Fünftel der Unternehmen haben solche Angriffe bereits spürbare – in einigen Fällen sogar massive – Schäden verursacht.

Abb. 3 – Wahrgenommenes Schadensrisiko durch Hacker-Angriffe
Wie groß ist das Risiko für Ihr Unternehmen, durch einen Hacker-Angriff gravierend geschädigt zu werden?



Auf 100 fehlende Prozent: unentschieden.

Das Risiko für das eigene Unternehmen, durch einen Cyber-Angriff gravierend geschädigt zu werden, bewertet rund die Hälfte der Befragten als (sehr oder eher) groß. Das Schadensrisiko wird nach einem Rückgang im letzten Jahr jetzt wieder deutlich höher bewertet. Die andere Hälfte bewertet das Risiko als (eher oder sehr) gering.

Anders die Bewertung derjenigen Befragten, deren Unternehmen bereits spürbare oder massive Schäden durch solche Angriffe erlitten haben: 70 Prozent sehen ein großes Risiko für gravierende Schäden. Im Vergleich: Nur rund 40 Prozent der Befragten aus Unternehmen, die in der Vergangenheit noch nicht mit den Auswirkungen von erfolgreichen Cyber-Attacken konfrontiert waren, sehen ein großes Risiko, dass zukünftige Angriffe zu gravierenden Schäden führen könnten.

Überdurchschnittlich häufig sehen Führungskräfte aus großen Unternehmen mit 1.000 und mehr Mitarbeitern hier hohe Schadensrisiken.

Das Schadensrisiko wird damit häufiger als in den beiden Vorjahren als sehr bzw. eher groß eingeschätzt und erreicht den zweithöchsten Wert seit Beginn der Messung durch den Cyber Security Report 2013.

„Unsere Erfahrungen zeigen, dass in Unternehmen, bei denen Cyber-Sicherheit einen hohen Stellenwert einnimmt, aktiv gemanagt sowie stets an Größe und Anforderungen des Unternehmens angepasst wird, ein IT-Angriff bisher keine (großen) Auswirkungen hatte."

Peter Wirnsperger, Cyber Risk Leader

2. Risikomanagement und Verantwortung

Das Thema Cyber-Sicherheit wird vor dem zuvor dargestellten Hintergrund wachsender Bedrohungen bei den Studienteilnehmern immer wichtiger: In gut zwei Dritteln der mittleren und großen Unternehmen hat es in den letzten Jahren sogar deutlich, in einem weiteren Viertel etwas an Bedeutung gewonnen. Besonders stark ist diese Entwicklung in großen Unternehmen mit 1.000 und mehr Mitarbeitern. Hier berichten 87 Prozent der Führungskräfte von einem deutlichen Bedeutungszuwachs.

Hauptgrund dafür ist die immer wichtigere Rolle, die die IT-Infrastruktur für die Unternehmen spielt. Zudem nehmen die Befragten vermehrt Angriffe auf andere Unternehmen wahr, eher noch als dass die Zunahme von Angriffen auf das eigene Unternehmen eine Rolle spielt. Für deutlich weniger Antwortgeber sind Änderungen von gesetzlichen Rahmenbedingungen ausschlaggebend für die Bedeutungszunahme des Themas Cyber-Sicherheit.

Gut ein Viertel der mittleren und großen Unternehmen räumt jedoch immer noch ein, dass es bei ihnen zur Identifikation und Bewertung von Cyber-Risiken keine definierten Prozesse gibt. Überdurchschnittlich häufig ist das in kleineren Unternehmen und im Handel der Fall.

Abb. 4 – Cyber-Sicherheit wird wichtiger – vor allem in großen Unternehmen
Das Thema Cyber-Sicherheit hat in den letzten Jahren im eigenen Unternehmen deutlich an Bedeutung gewonnen.

Abb. 5 – Prozesse zur Identifikation und Bewertung von Cyber-Risiken

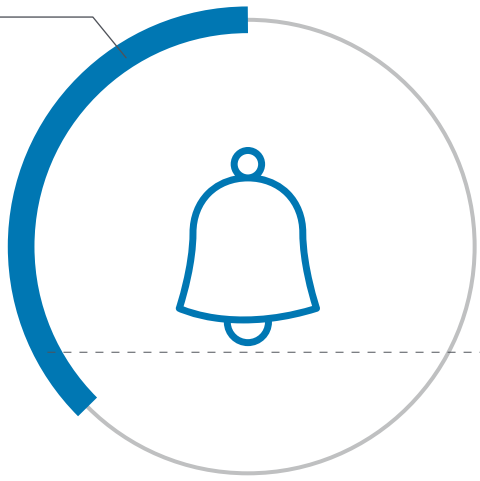
71%

der Unternehmen insgesamt haben **definierte Prozesse,** wie Cyber-Risiken identifiziert und bewertet werden.

Abb. 6 – Information der Führungsebene über den Stand der Cyber-Sicherheit

In 37%

der Unternehmen wird die Führungsebene über den Stand der Cyber-Sicherheit im Unternehmen **nur anlassbezogen informiert.**



In 33%

der **Unternehmen mit 1.000 und mehr Mitarbeitern** wird die Führungsebene über den Stand der Cyber-Sicherheit im Unternehmen nur anlassbezogen informiert.

Auch der Formalisierungsgrad der Instrumente, mit denen der Stand der Cyber-Sicherheit im eigenen Unternehmen dokumentiert und überwacht wird, ist häufig gering. Nur 11 Prozent der Befragten nutzen dafür definierte Kennzahlen, 15 Prozent ein Ampelsystem. Die große Mehrheit – auch unter den großen Unternehmen – setzt auf (mündliche oder schriftliche) Berichte.

Bei 37 Prozent der Teilnehmer wird die Führungsebene ausschließlich anlassbezogen über den Stand der Cyber-Sicherheit im eigenen Unternehmen informiert, bei nur rund einem Viertel passiert das fortlaufend. In dieser Frage bestehen auch nur begrenzte Unterschiede zwischen größeren und kleineren Unternehmen.

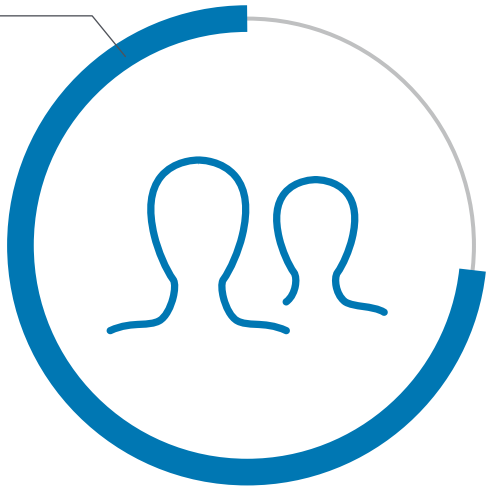
Die Führungskräfte ihrerseits müssen sich beim Thema IT-Sicherheit zu rund drei Vierteln auf das verlassen, was ihnen ihre Experten raten, und räumen ein, dass sie bei dem Thema kaum in der Lage sind, sich eigenständig ein Urteil zu bilden.

Die Verantwortung für den Bereich Cyber-Sicherheit verorten Führungskräfte im eigenen Unternehmen jeweils fast zur Hälfte auf der operativen Ebene, also im Bereich IT beziehungsweise Infrastruktur, und auf der Geschäftsführungs- beziehungsweise Vorstandsebene, kaum dagegen im Bereich Risikomanagement.

Abb. 7 – Führungskräfte sind auf Experten angewiesen

73%

der Führungskräfte **verlassen sich auf den Rat von Experten,** wenn es um das Thema IT-Sicherheit geht.



„Cyber-Risiken sind zu einem permanenten und wesentlichen Unternehmensrisiko geworden. Daher muss das Management dieser Risiken selbstverständlicher und integraler Bestandteil der Risikosteuerung auf Gesamtunternehmensebene sein."

Katrin Rohmann, Government & Public Services Leader

„Erfolgreiches Management von Cyber-Risiken erfordert ein gutes Zusammenspiel zwischen Experten und Unternehmensführung. Standardisierte und etablierte Prozesse und Berichtswege können dies effektiv gestalten."

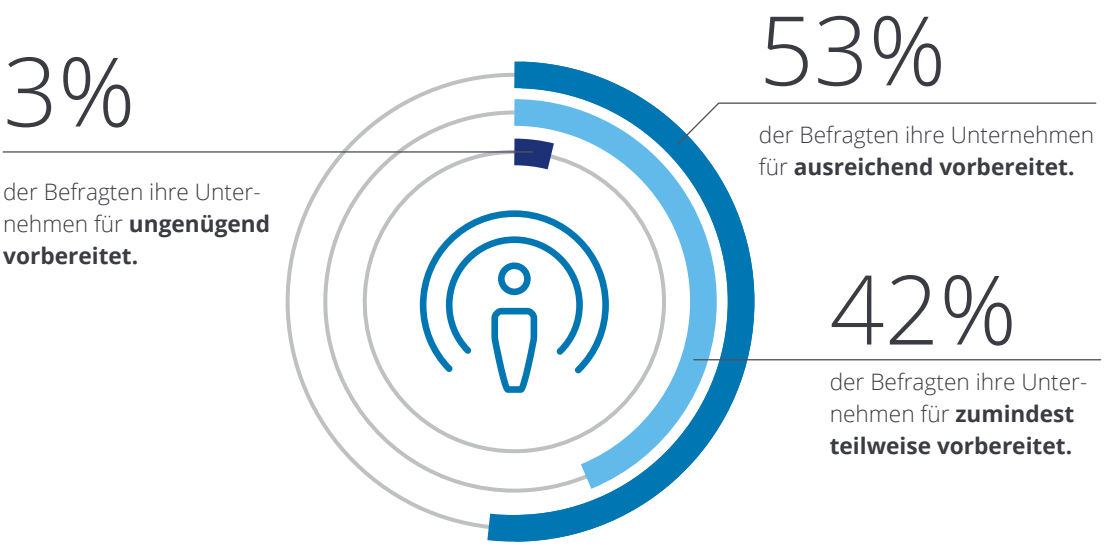
Peter Wirnsperger, Cyber Risk Leader

3. Resilienz und Maßnahmen zum Schutz

Cyber-Kriminelle werden professioneller und sie nutzen vermehrt neueste Technologien, um vorhandene Schutzmechanismen zu umgehen. Gleichzeitig werden Unternehmen und ihre Produkte immer digitaler, dadurch entstehen stets neue Angriffsvektoren. Während die Methoden der Cyber-Kriminellen immer ausgeklügelter und komplexer werden, stellt sich die Frage, ob die Unternehmen ihre Abwehrfähigkeiten im gleichen Maße aufrüsten.

Wie gut vorbereitet halten die Befragten ihre Unternehmen, um auf erfolgreiche Angriffe angemessen zu reagieren? Hier gab es eine ausgewogene Einschätzung: Etwas mehr als die Hälfte der Befragten hält ihr Unternehmen für ausreichend vorbereitet um – nach einem erfolgreichen Eindringversuch – die Folgen einzudämmen und die Schäden zu minimieren. 42 Prozent der Befragten halten ihr Unternehmen für zumindest teilweise, nur 3 Prozent für ungenügend vorbereitet.

Abb. 8 – Ausreichende Resilienz?
Um auf Angriffe angemessen zu reagieren, halten …

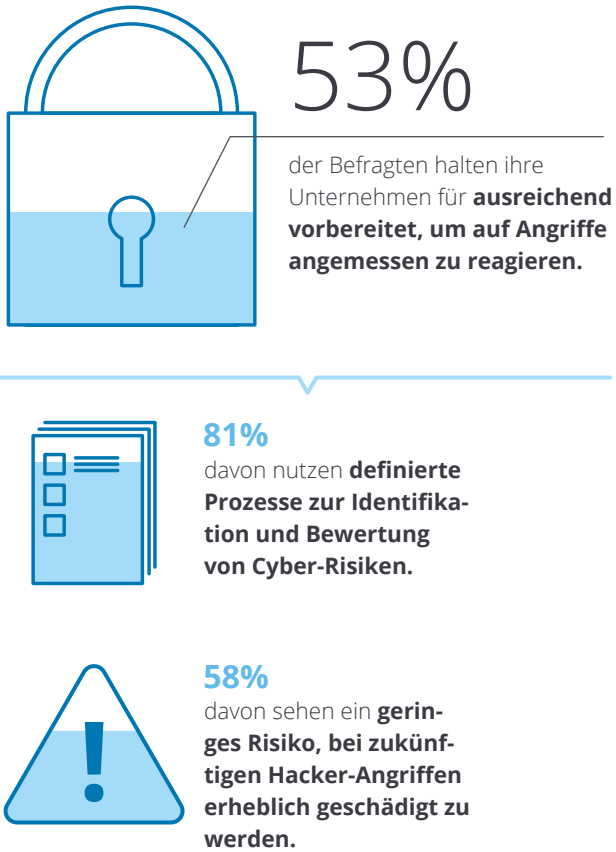


Ein naheliegender Zusammenhang besteht zwischen den Einschätzungen des Schadensrisikos und der Abwehrfähigkeit. Diejenigen Befragten, die ihr Unternehmen für ausreichend vorbereitet sehen, bewerten das Risiko, aus zukünftigen Angriffen einen Schaden zu erleiden, eher als gering. Außerdem kommen in der Teilgruppe, die ihre Unternehmen als ausreichend vorbereitet einschätzt, auch weitaus häufiger definierte Prozesse zur Identifikation und Bewertung von Cyber-Risiken zur Anwendung.

Zwischen der Einschätzung des Schadensrisikos und dem Formalisierungsgrad bei der Dokumentation und Überwachung von Cyber-Risiken besteht hingegen kein signifikanter Zusammenhang, also z.B. dahingehend, dass eine hohe Risikoerwartung mit einer formelleren Risikoüberwachung einhergehen würde.

Allerdings gibt es eine signifikante Korrelation zwischen der Art der Berichterstattung zu Cyber-Risiken und der Kompetenzeinschätzung der befragten Führungskräfte für Cyber-Security: Diejenigen von ihnen, die sich bei diesem Thema – nach eigener Aussage – auf das verlassen müssen, was ihnen Experten raten, nutzen überproportional mündliche oder schriftliche Berichte. Ampelsysteme und definierte Kennzahlen hingegen kommen häufiger zu Anwendung bei denjenigen Führungskräften, die sich als weniger abhängig von Experten sehen, als bei der Gesamtgruppe der Befragten.

Abb. 9 – Geringes Risiko durch definierte Prozesse



Exkurs: Unsere Befragung von CISOs

In diesem Jahr haben wir, ergänzend zu der repräsentativen Befragung von Führungskräften, Kurzinterviews mit Sicherheitsverantwortlichen, zumeist den Chief Information Security Officers (CISOs), aus Unternehmen geführt. In den über 20 Interviews mit Vertretern aus den Sektoren Consumer Products, Energy, Resources & Industrials, Financial Services, Life Sciences & Health Care und Technology, Media & Telecom wollten wir auch die Sicht der Experten zu ausgewählten Themenbereichen unserer Studie angemessen abbilden und mögliche Unterschiede im Sicherheits- und Risikoverständnis identifizieren. In den Kurzinterviews haben wir unseren Gesprächspartnern sechs Fragen zu den Themenbereichen Cyber-Risiken, Governance und Resilienz gestellt. Im Folgenden stellen wir wesentliche Erkenntnisse und Aussagen dar.

Risiken

Welche Fähigkeiten muss ein Unternehmen haben, um das Risiko durch Cyber-Angriffe zu minimieren?
Auch wenn unsere Gesprächspartner unterschiedliche Schwerpunkte genannt haben, hoben alle Interviewpartner hervor, dass nur eine Kombination verschiedener Fähigkeiten einen dauerhaften Schutz vor Cyber-Angriffen garantiert: Awareness und Training, Identifikation der Bedrohungen, angemessenes Risikomanagement, technische Maßnahmen und die Fähigkeit zur wirksamen Reaktion auf laufende Angriffe. Auffällig war aus unserer Sicht der hohe Stellenwert, den die Befragten dabei der Awareness aller Mitarbeiter beimaßen – also der Forderung, dass alle Mitarbeiter ein Verständnis für Cyber-Risiken und ihre persönliche Verantwortung in diesem Zusammenhang haben sollten.

Inwieweit unterscheiden sich Cyber-Risiken von anderen Risiken, mit denen Unternehmen konfrontiert sind?
Drei Merkmale sind aus Sicht unserer Interviewpartner charakteristisch für Cyber-Risiken im Vergleich zu anderen Sicherheitsrisiken: zunächst die Skalierbarkeit von Angriffen. Das heißt in diesem Zusammenhang: Cyber-Angriffe sind relativ kostengünstig, können aus der Distanz ausgeführt werden und sind einfach anzupassen und zu wiederholen. Ein zweites Merkmal ist die Schwierigkeit, Cyber-Angriffe zu bemerken; in ihrer Vorbereitung, während der Ausführung oder sogar nach einem erfolgreichen Angriff. Als drittes Merkmal werden die potenziellen Schäden erfolgreicher Attacken genannt. Cyber-Angriffe lassen sich nach Einschätzung der Befragten schwerer in ihrer Reichweite und Dauer eingrenzen als andere Angriffe.

Ein Gesprächspartner hat ergänzend die Herausforderung angesprochen, Cyber-Risiken mit den Methoden des klassischen Risikomanagements, also hinsichtlich ihrer Eintrittswahrscheinlichkeit und Schadenshöhe zu erfassen.

Governance

Welche Verantwortung und Aufgaben sehen Sie auf der Führungsebene von Unternehmen für Cyber-Security?
Die Geschäftsführung oder der Vorstand sollte aus Sicht unserer Interviewpartner die Rahmenbedingungen für die Cyber-Strategie des Unternehmens definieren und die Umsetzung der entsprechenden Maßnahmen – beispielsweise durch die Bereitstellung des erforderlichen Budgets und die Schaffung organisatorischer Voraussetzungen – ermöglichen. Häufig angesprochen wurde abermals die Notwendigkeit von „Awareness" speziell auf der Führungsebene, also einem Bewusstsein und Verständnis für Cyber-Sicherheit von Vorstand oder Geschäftsführung.

Wie im vorigen Kapitel angesprochen, sehen Führungskräfte aller Ebenen und Branchen diese Verantwortung jedoch nur zu rund der Hälfte überhaupt bei der Führungsebene bzw. dem Vorstand.

Wie sollten Cyber-Risiken für ein Unternehmen identifiziert und bewertet werden? Also z.B. durch definierte Kennzahlen, ein Ampelsystem oder mündliche/schriftliche Berichte?
Auf diese Frage haben wir sehr unterschiedliche Antworten erhalten. Viele der interviewten CISOs nutzen in ihren Unternehmen vorwiegend mündliche oder schriftliche Berichte. Diese Aussage deckt sich mit den Ergebnissen der Umfrage: Drei Viertel der Führungskräfte haben ebenso geantwortet. Interessant war jedoch die Begründung der CISOs. Berichte ermöglichen es aus ihrer Sicht zum einen besser, die spezifischen Herausforderungen von Cyber-Risiken gegenüber der Führungsebene zu verdeutlichen und eine angemessene Awareness zu schaffen. Zum anderen sehen einige CISOs Schwierigkeiten, aussagekräftige Kennzahlen zu definieren, die ein Management der Cyber-Risiken ermöglichen. Bei einigen der Interviewten kommen hingegen bewusst ausgewählte Kennzahlen im Sinne eines Cyber-Risiko-Cockpits zur Anwendung und Berichte spielen eine nachrangige Rolle. Dies geschieht dann mit dem Ziel, diese Gefährdungen in ein unternehmensweites Risikomanagement einzubinden. Unabhängig von der aktuellen Vorgehensweise halten die meisten der Befragten aber eine Kombination von ausgewählten Kennzahlen und daran anknüpfenden Berichten für den richtigen Ansatz zur Identifikation und Bewertung von Cyber-Risiken.

Resilienz

Staatliche Stellen, Dienstleister, aber auch Fachverbände und andere Gremien sprechen immer öfter von Cyber-Resilienz. Ist das ein Begriff, der für Sie eine Bedeutung hat? Falls ja, was verstehen Sie darunter?

Was sind aus Ihrer Sicht die wesentlichen Voraussetzungen für Cyber-Resilienz?
In unseren letzten beiden Fragen ging es um „Cyber-Resilienz". Ein Großteil der Befragten assoziiert mit diesem Begriff Widerstandsfähigkeit. Resilient ist ein Unternehmen, wenn es in der Lage ist, Cyber-Angriffe abzuwehren und durch gezielte Gegenmaßnahmen Schäden einzugrenzen. Diese Fähigkeit ist für die Befragten erstrebenswert, allerdings kommt der Begriff Cyber-Resilienz nur bei einem Teil der Unternehmen zur Anwendung. Bei anderen wiederum ist sie als strategisches Ziel der Cyber-Security explizit definiert. Auch wenn wir nicht bewusst danach gefragt haben, gab es auch interessante Aussagen zu dem Bezugspunkt: Wer oder was ist resilient? Resilienz kann demnach sowohl eine Fähigkeit einer einzelnen Person, eines Unternehmens, einer komplexen Lieferkette oder sogar eines Staates sein.

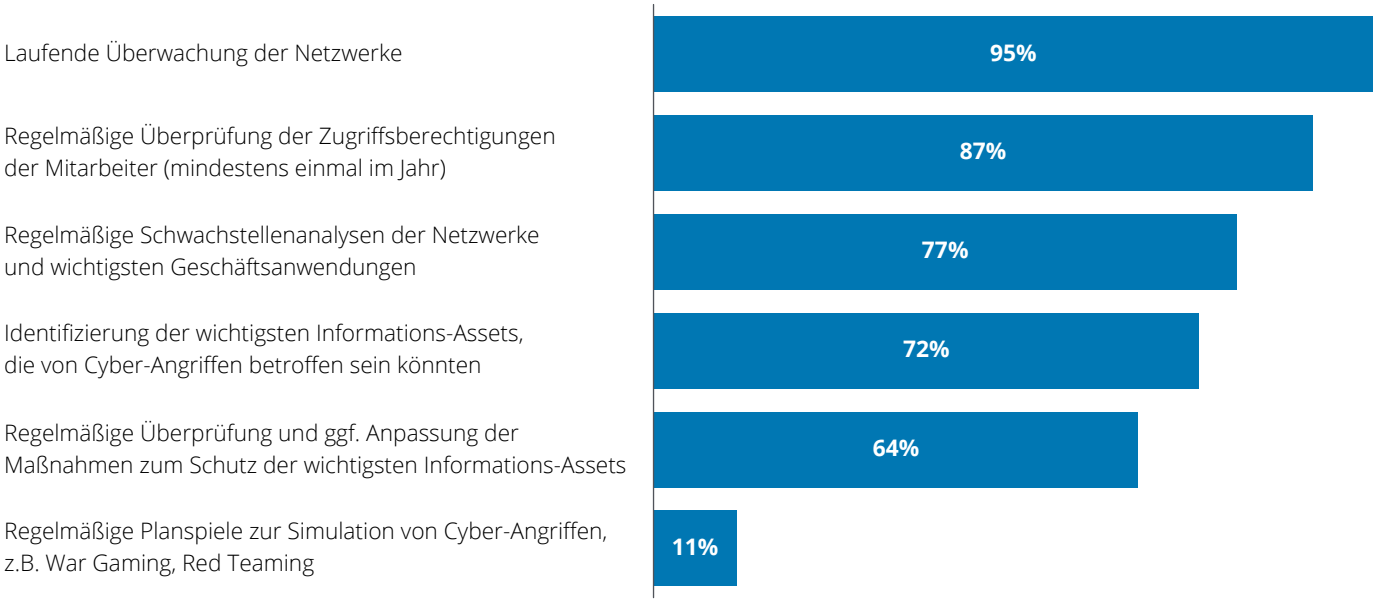
Wir bewerten zusammenfassend: Cyber-Resilienz wird als eine erstrebenswerte Fähigkeit verstanden. Der Begriff eignet sich zur Umschreibung der verschiedenen Fähigkeiten, die ein Unternehmen besitzen muss, um der Herausforderung durch Cyber-Angriffe angemessen begegnen zu können. Allerdings gibt es derzeit noch Definitionsbedarf, was Cyber-Resilienz eigentlich genau ausmacht und wie diese abstrakte Fähigkeit systematisch bewertet und verbessert werden kann.

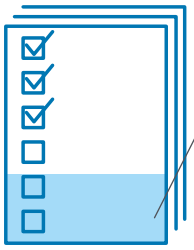
Auch haben wir in diesem Jahr wieder Fragen zu den konkreten Maßnahmen, die Unternehmen angesichts der Cyber-Risiken ergreifen, gestellt.

Zum Schutz ihrer IT-Infrastruktur überwachen fast alle Unternehmen laufend ihre Netzwerke, 87 Prozent überprüfen regelmäßig die Zugriffsberechtigungen ihrer Mitarbeiter. Ihre wichtigsten Informations-Assets haben allerdings nur 72 Prozent der Interviewten identifiziert, nur 64 Prozent überprüfen auch regelmäßig die Maßnahmen zum Schutz dieser Assets und passen sie gegebenenfalls an. Regelmäßige Simulationen von Cyber-Angriffen (z.B. durch Red Teaming oder im Rahmen von War Games) führen lediglich 11 Prozent der Unternehmen durch. Insgesamt bewegen sich die Antworten damit auf dem Niveau des Vorjahres.

Während also 85 Prozent der Befragten angaben, dass ihr Unternehmen Cyber-Angriffen ausgesetzt ist, und es bei 21 Prozent spürbare oder massive Schäden gab, simuliert nur rund jedes zehnte Unternehmen derartige Angriffe.

Abb. 10 – Maßnahmen zum Schutz der IT-Infrastruktur
Die Unternehmen haben folgende Maßnahmen zum Schutz ihrer IT-Infrastruktur ergriffen bzw. durchgeführt:





32%

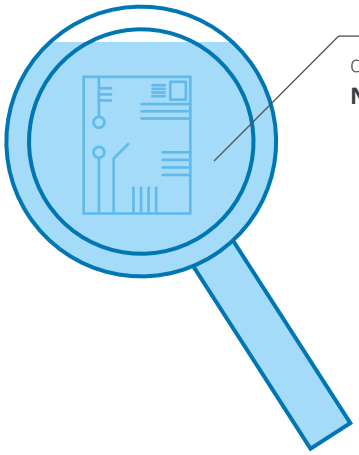
der Unternehmen führen **höchstens drei der sechs** genannten Maßnahmen durch.

Und auch wenn 95 Prozent der Unternehmen ihre Netzwerke laufend überwachen, erhalten nur rund drei Viertel der Führungskräfte dazu auch regelmäßig Berichte.

Rund drei Viertel der Befragten lassen sich darüber hinaus regelmäßig von externen Spezialisten zu aktuellen Entwicklungen im Bereich Cyber-Security beraten, 68 Prozent haben externe Dienstleister beauftragt, sich um dieses Thema in ihrem Unternehmen zu kümmern.

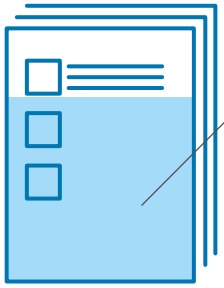
Lieferanten werden von rund jedem zweiten Studienteilnehmer auf die Einhaltung von IT-Sicherheitsstandards verpflichtet. Große Unternehmen – und zwar zwei Drittel derselben – fordern dies von ihren Lieferanten deutlich öfter.

Abb. 11 – Monitoring und Reporting



95%

der Unternehmen **überwachen ihre Netzwerke laufend.**



73%

der Führungskräfte erhalten regelmäßig **Berichte über mögliche Angriffe** auf das Netzwerk.

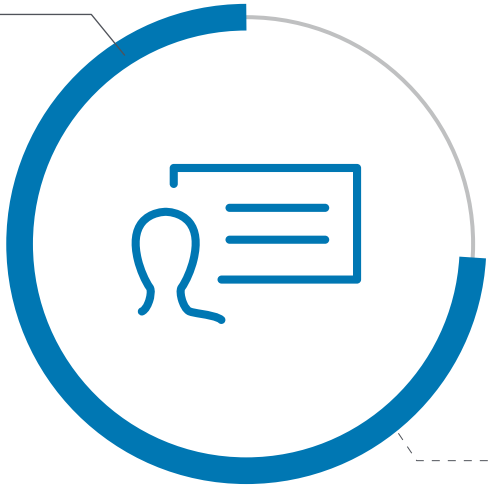
„Mehr als acht von zehn der Unternehmen sind regelmäßigen Cyber-Angriffen ausgesetzt, bei zwei von zehn Organisationen hat das schon zu deutlichen Schäden geführt, aber nur jedes zehnte Unternehmen bereitet sich durch simulierte Angriffe darauf vor. Die Verantwortlichen glauben anscheinend noch nicht daran, dass solche Krisenübungen ihre Sicherheit wirksam erhöhen."

Peter Wirnsperger, Cyber Risk Leader

Abb. 12 – Nicht-technische Maßnahmen zum Schutz der IT-Infrastruktur: Beratung und externe Dienstleister

74%

der Unternehmen insgesamt



83%

der Unternehmen mit 1.000 und mehr Mitarbeitern

... lassen sich **regelmäßig von externen Spezialisten beraten,** welche aktuellen Entwicklungen es im Bereich Cyber-Security gibt und wie sie sich am besten darauf einstellen.

68%

der Unternehmen insgesamt

68%

der Unternehmen mit 1.000 und mehr Mitarbeitern

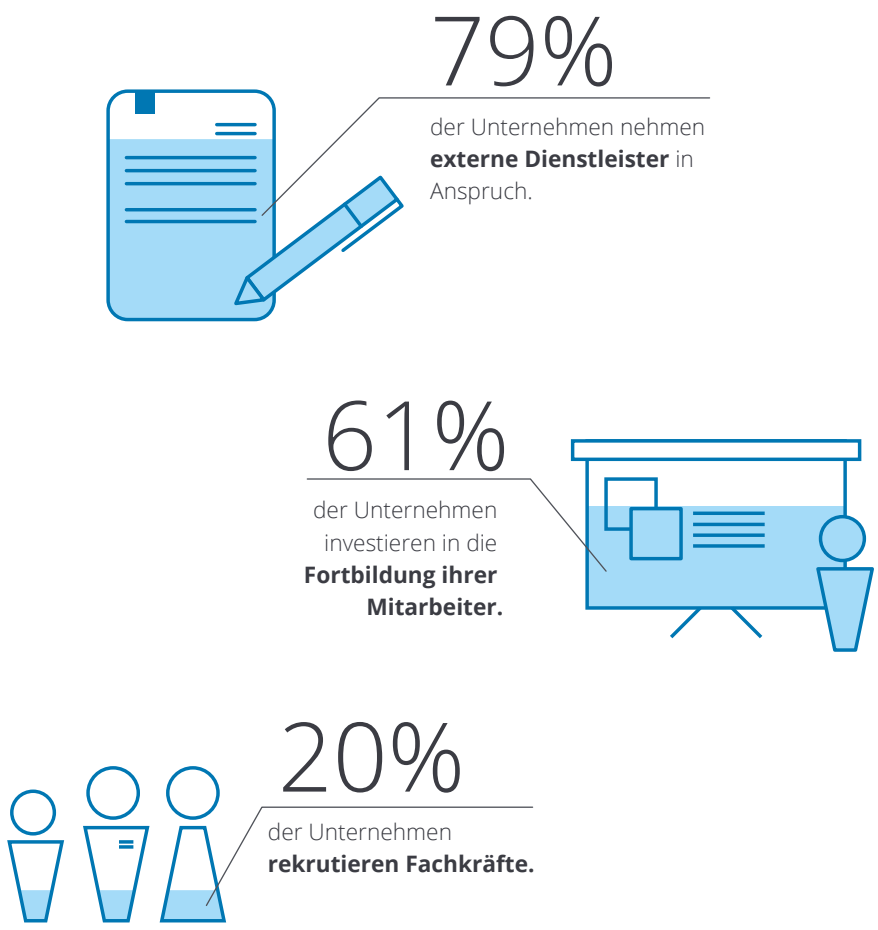
... haben **externe Dienstleister beauftragt,** die sich um das Thema Cyber-Security kümmern, nutzen also bspw. sogenannte **Managed Security Services.**

4. Fachkräfte für die Sicherheit

In der Vergangenheit wurde Cyber-Sicherheit als Mittel zum Schutz von Informationen, zum Beispiel von Finanzdaten, geistigem Eigentum oder auch personenbezogene Daten, angesehen. Fast selbstverständlich wurden Themen mit Cyber-Bezug in der Abteilung Informationstechnologie, die althergebracht mit der Verwaltung und dem Schutz von Informationen betraut war, verortet.

Führungskräfte in der Wirtschaft sehen immer deutlicher, dass das Thema Cyber nicht nur eine Aufgabe der IT-Abteilung ist. Angesichts der fortschreitenden Digitalisierung von Geschäftsprozessen erkennen sie Herausforderungen für alle Geschäftsbereiche. Insbesondere der Personalbereich steht vor der großen Aufgabe, den Bedarf an IT-Fachkräften angemessen zu decken. 64 Prozent der deutschen Unternehmen geben an, Probleme bei der Gewinnung von IT-Fachkräften zu haben.[1] Dazu gehören auch Expertinnen und Experten der IT-Sicherheit. Um eine ausreichende Expertise in diesem Bereich im eigenen Unternehmen sicherzustellen, setzen Führungskräfte vor allem auf externe Dienstleister und die Fortbildung ihrer Mitarbeiter. Die Rekrutierung von entsprechend qualifizierten Fachkräften ist dagegen nur für 20 Prozent ein wesentlicher Baustein.

Abb. 13 – Quelle des Know-hows im Bereich IT-Sicherheit in Unternehmen



[1] Statistisches Bundesamt (2019).

Unabhängig vom Wirtschaftssektor ist erkennbar, dass kleinere Unternehmen deutlich weniger Fachkräfte auf dem Arbeitsmarkt rekrutieren als größere. Im direkten Vergleich heißt das, dass Unternehmen ab 1.000 Mitarbeitern zu 38 Prozent die benötigte Expertise am Markt rekrutieren und Unternehmen bis 249 Mitarbeiter nur zu 11 Prozent.

Dennoch berichtet gut ein Drittel der mittleren und großen Unternehmen von größeren Schwierigkeiten, ausreichend Fachkräfte für den Bereich IT-Sicherheit zu finden, von den Unternehmen ab 1.000 Mitarbeitern rund die Hälfte. Mehr als die Hälfte der Führungskräfte von Unternehmen bis 249 Mitarbeitern berichtet dagegen davon, dass sie im Bereich der IT-Sicherheit keinen Fachkräftemangel haben.

Den größten Handlungsbedarf, um sicherzustellen, dass auch in Zukunft ausreichend Fachkräfte in diesem Bereich zur Verfügung stehen, sehen Wirtschaftsführer eher bei sich als beim Staat: Nur 15 Prozent finden, es ist hier vor allem der Staat gefragt, der Studiengänge und Ausbildungsinhalte entsprechend anpassen sollte, 40 Prozent sehen dagegen die Unternehmen in der Pflicht, ihre Mitarbeiter durch Schulungen und Fortbildungen entsprechend zu qualifizieren, und 43 Prozent sehen Staat und Wirtschaft gleichermaßen gefordert. Von den Abgeordneten sieht sogar die Mehrheit beide Akteure gleichermaßen in der Pflicht.

Abb. 14 – Probleme bei der Suche nach Fachkräften
Ausreichend Fachkräfte für den Bereich IT-Sicherheit zu finden, stellt für...

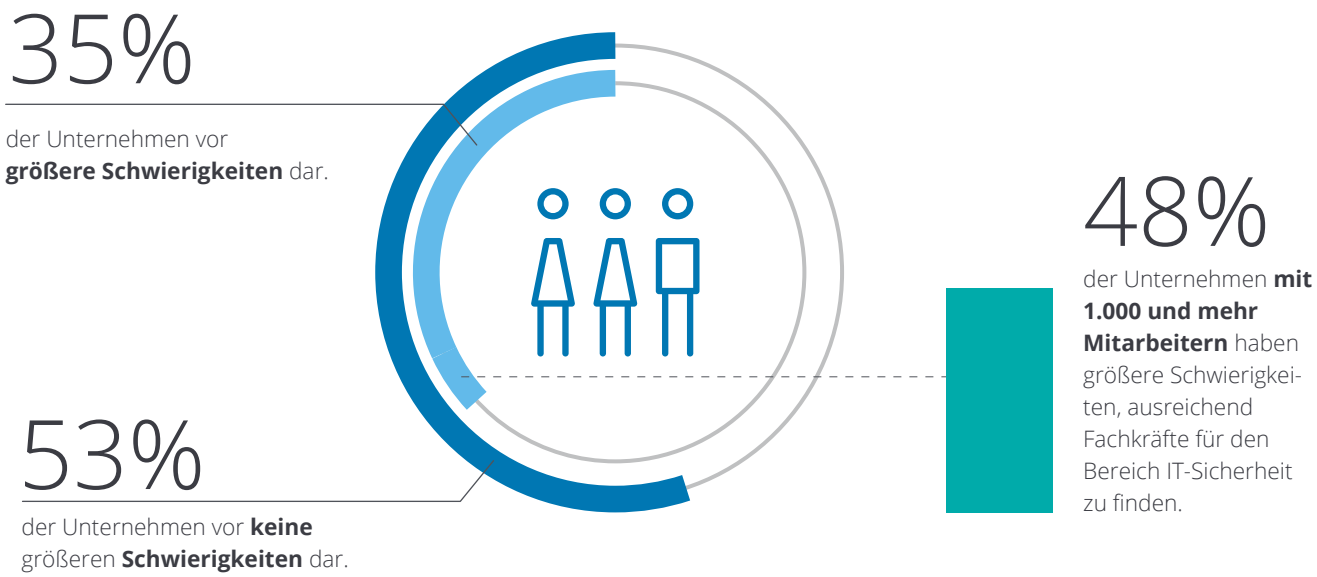
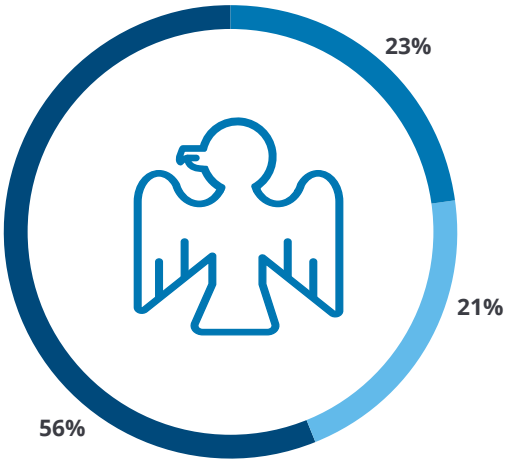
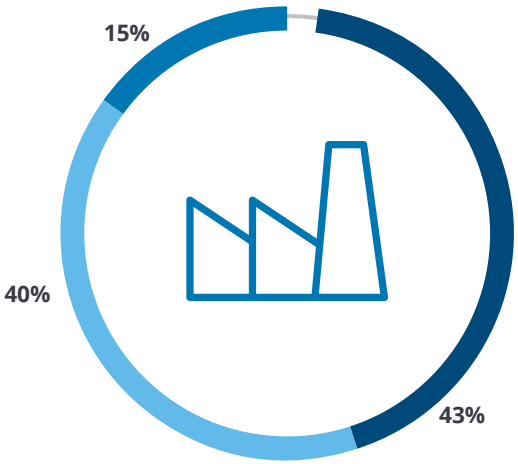


Abb. 15 – Handlungsbedarf von Staat und Wirtschaft
Der größte Handlungsbedarf, um sicherzustellen, dass auch in Zukunft ausreichend Fachkräfte für den Bereich IT-Sicherheit zur Verfügung stehen, besteht …

aus Sicht der Abgeordneten … **aus Sicht der Wirtschaftsführer …**

… beim Staat, der Studiengänge und Ausbildungsinhalte entsprechend anpassen sollte.
… bei den Unternehmen, die ihre Mitarbeiter durch Schulungen und Fortbildungen entsprechend qualifizieren sollten.
… bei beiden gleichermaßen.





Auf 100 fehlende Prozent: unentschieden.

„Führungskräfte in Politik und Wirtschaft müssen gleichermaßen sicherstellen, dass im Staat und in Unternehmen auch in Zukunft ausreichend Fachkräfte für den Bereich Cyber-Sicherheit zur Verfügung stehen. Kompetenzzentren und Expertenpools können zur Deckung des Fachkräftebedarfs nachhaltig beitragen."

Katrin Rohmann, Government & Public Services Leader

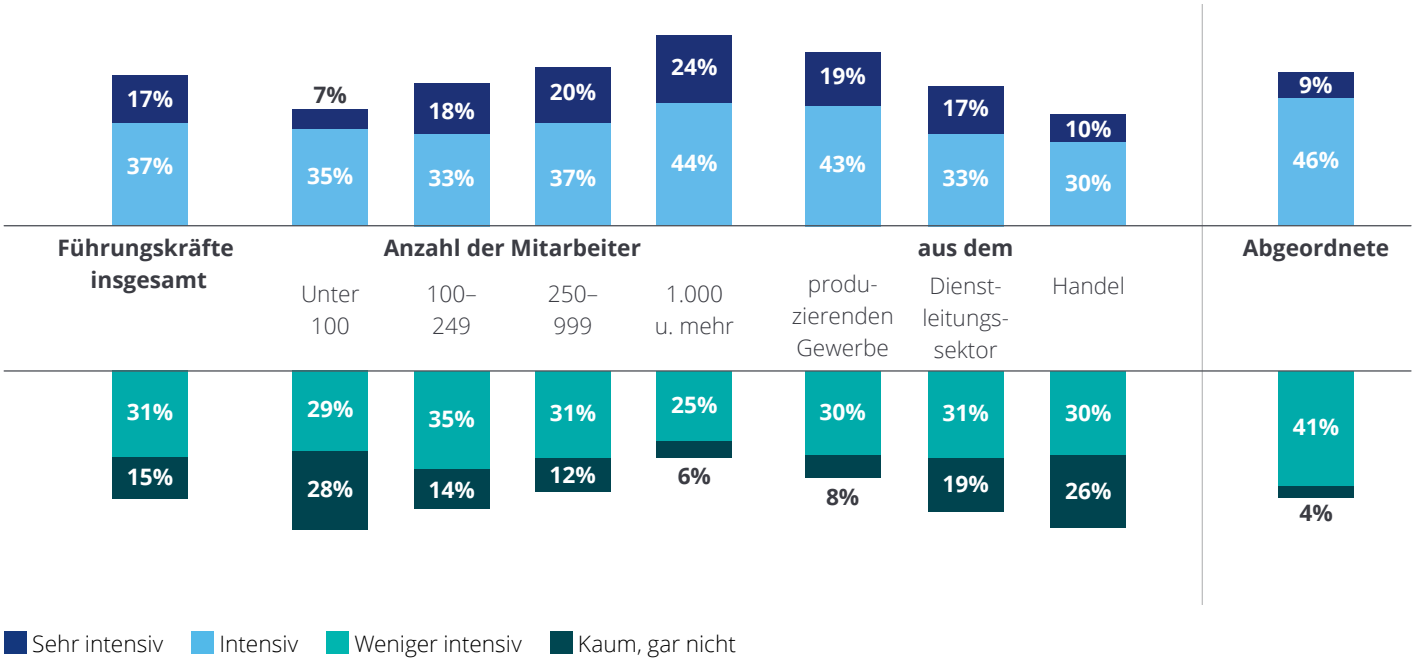
5. Neue Anforderungen durch Industrie 4.0

Industrie 4.0 wird häufig als Serie disruptiver Innovationen in der Produktion und Umwälzungen industrieller Prozesse bezeichnet, die höhere Produktivität versprechen.

Diese fundamentale Umgestaltung von industriellen Produktionsprozessen beinhaltet, dass einzelne Maschinen, Geräte und Produkte vermehrt durch das Internet verbunden sind und autonom über die Produktionskette hinweg kommunizieren können. Durch diese Vernetzung können nicht nur Daten effizient ausgetauscht werden, sondern Maschinen können sich auch unabhängig selbst steuern und Prozesse veranlassen. Diese Transformation des produzierenden Gewerbes wird oft als Industrie 4.0 bezeichnet, da sie – ähnlich wie drei vorangegangene Umwälzungen durch Dampfkraft, Elektrizität und Informationstechnologie – ein hohes Potenzial an Effizienzsteigerung in Aussicht stellt.

Industrie 4.0 wird auf politischer Ebene als Chance für den Industriestandort Deutschland gesehen und somit fokussieren sich politische Initiativen seit einigen Jahren auf deren Förderung. Zum Beispiel zielt das Zukunftsprojekt „Industrie 4.0" des Bundesministeriums für Forschung und Bildung (BMFB) darauf ab, die deutsche Industrie für die Zukunft der Produktion zu rüsten. Dabei wird nicht nur auf Forschung und Weiterbildungsmaßnahmen gesetzt, sondern Unternehmen werden auch praktische Handlungsempfehlungen an die Hand gegeben. Während produzierende deutsche Unternehmen

Abb. 16 – Auseinandersetzung mit dem Thema Industrie 4.0



Auf 100 fehlende Prozent: unentschieden.

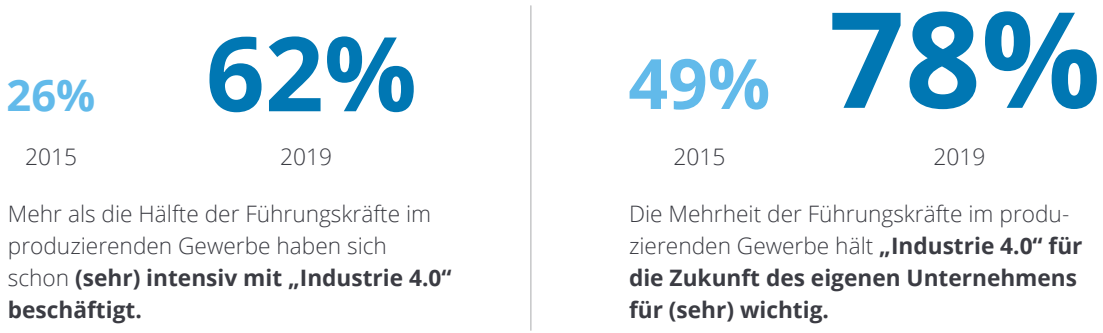
der Industrie 4.0 einen hohen Stellenwert beimessen, stehen diese Unternehmen vor einigen Herausforderungen bei der Umsetzung.

Insgesamt hat sich bisher nur knapp mehr als die Hälfte der Führungskräfte intensiv oder sehr intensiv mit dem Thema Industrie 4.0 auseinandergesetzt, während sich knapp weniger als die Hälfte weniger intensiv oder kaum mit dem Thema beschäftigt haben. Ähnlich sieht es bei Abgeordneten aus, von denen 55 Prozent angegeben haben, dass sie sich (sehr) intensiv, und 45 Prozent, dass sie sich weniger intensiv oder kaum mit dem Thema auseinandergesetzt haben.

Es gibt eine Korrelation zwischen der Größe des Unternehmens und der Reflexion mit dem Thema: Je kleiner ein Unternehmen ist, desto weniger intensiv beschäftigen sich dessen Führungskräfte mit Industrie 4.0.

Im Vergleich zum allgemeinen Stimmungsbild unter Führungskräften ist im produzierenden Gewerbe die Anzahl der Unternehmen, die das Thema intensiv oder sehr intensiv reflektiert haben, höher und liegt bei 62 Prozent. Im Vergleich zu den Vorjahren kann ein deutlicher Zuwachs an Führungskräften festgestellt werden, die sich mit Industrie 4.0 (sehr) intensiv beschäftigt haben. Während deren Anteil im Jahr 2015 nur bei 26 Prozent lag, waren es im Jahre 2018 schon 49 und sind es nunmehr 62 Prozent. Zusätzlich wird auch die Bedeutung des Themas für das eigene Unternehmen zunehmend höher veranschlagt. So lag im Jahr 2015 der Wert bei 49 Prozent, wuchs 2018 auf 70 und 2019 auf 78 Prozent. Die Diskrepanz zwischen dem Stellenwert, den Führungskräfte Industrie 4.0 für ihr Unternehmen beimessen, und der Beschäftigung mit dem Thema ist hierbei ein interessanter Befund.

Abb. 17 – Zunehmende Bedeutung von Industrie 4.0 im produzierenden Gewerbe

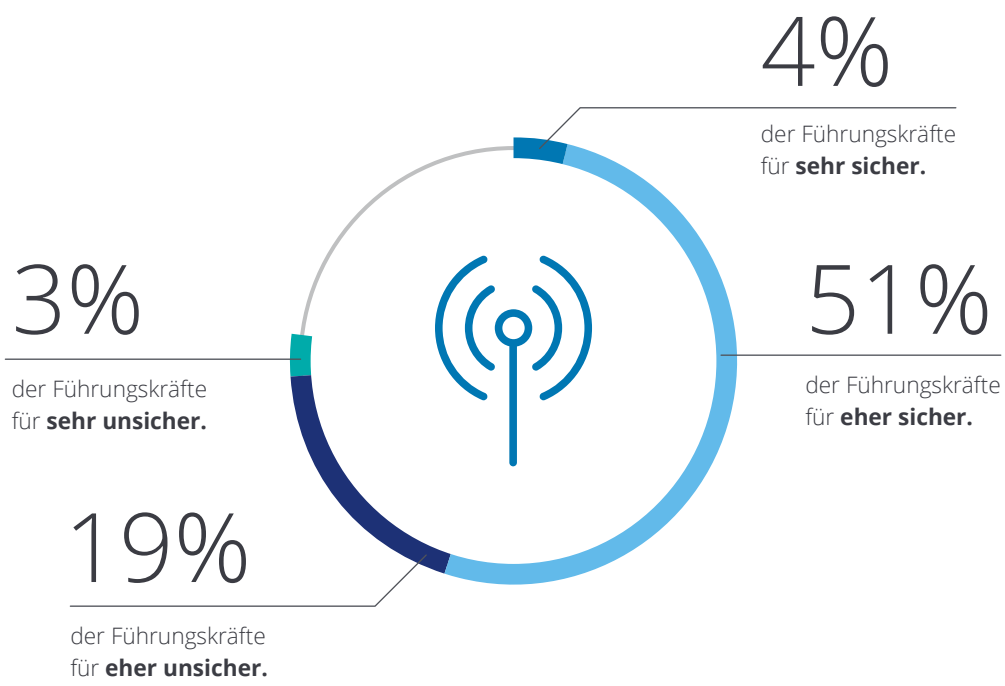


Nur eine Minderheit der Wirtschaftsführer äußert Bedenken in Bezug auf die Sicherheit bei der Nutzung des 5G-Standards zur Vernetzung von Produktionsabläufen. Lediglich 19 Prozent halten den Standard für eher unsicher, 3 Prozent für sehr unsicher. Gleichzeitig bewerten ihn 51 Prozent der Führungskräfte als eher sicher und 4 Prozent als sehr sicher.

„Es ist bereits viel auf den Weg gebracht, um Rahmenbedingungen für Schlüsseltechnologien in Deutschland zu schaffen. Es gilt nun herauszufinden, welche Unterstützung der Wirtschaft konkret erforderlich ist, um die Wettbewerbsfähigkeit hoch zu halten."

Katrin Rohmann, Government & Public Services Leader

Abb. 18 – Der Sicherheitsaspekt bei der Nutzung des 5G-Standards in der Produktion
Zur Vernetzung der Produktionsabläufe den 5G-Standard zu verwenden, halten ...

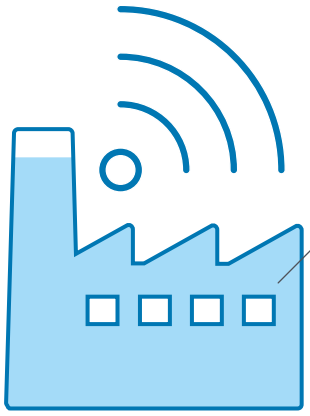


Auf 100 fehlende Prozent: unentschieden.

2019 berichten nur 28 Prozent der Führungskräfte, die sich mit dem Thema Industrie 4.0 näher beschäftigt haben, davon, dass sich die Cyber-Security-Strategie ihres Unternehmens in diesem Zusammenhang deutlich verändert hat oder verändern wird. 48 Prozent sehen hier kleinere, 11 Prozent gar keine Veränderungen. Dies ist ein beachtlicher Befund, da im Cyber Security Report 2018 Führungskräfte mit einer großen Mehrheit das Risiko von Cyber-Angriffen durch die Industrie-4.0-Entwicklung als steigend bewerteten. So gaben 83 Prozent der Wirtschaftsführer und 75 Prozent der Abgeordneten an, dass das Risiko von Cyber-Angriffen mit der Umsetzung von Industrie 4.0 und der Vernetzung von Produktionsprozessen steigt.[2]

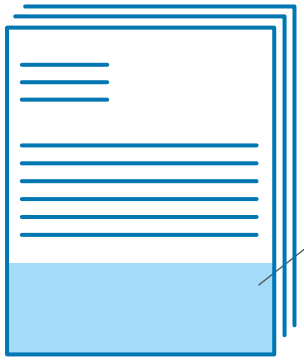
Zusammenfassend ist im Vergleich zu den Vorjahren festzustellen, dass Führungskräfte in Industrie 4.0 eine steigende Bedeutung für die eigenen Unternehmen sehen. Diese Ergebnisse weisen allerdings eine Diskrepanz zu den Maßnahmen auf, die Firmen ergreifen. Dies bezieht sich sowohl auf die direkte Beschäftigung mit dem Thema als auch auf das Anpassen der Cyber-Security-Strategien an die Risiken, die Industrie 4.0 mitbringen kann.

Abb. 19 – Auswirkungen von Industrie 4.0 auf die Cyber-Security-Strategie



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.

[2] Deloitte, Cyber Security Report 2018.

Handlungsfelder

Der voranschreitende technologische Wandel und die verbindende Kraft der Digitalisierung benötigen eine Cyber-Sicherheit der nächsten Generation, um beim Wachstum von Unternehmen zu helfen und Cyber-Resilienz von Organisationen von innen heraus zu stärken.

Verantwortung

Sensibilisierung und Eigenverantwortung sind neben technischen Lösungen und dem Expertenrat notwendige Führungsmittel, um mit der zunehmenden Bedrohung durch Cyber-Risiken umzugehen. Ein Managementsystem für Informationssicherheit legt dabei Verfahren und Regeln in einer Organisation fest. Es dient dazu, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren und fortlaufend aufrechtzuerhalten. Die Verantwortung hierfür ist „Chefsache“ und die Einbindung ins Risikomanagement des Unternehmens bedeutend.

Resilienz und Maßnahmen zum Schutz

Um Cyber-Sicherheit erfolgreich gewährleisten zu können, ist die umfassende Resilienz ein wesentlicher Aspekt. Der erste Schritt zu einer hohen organisationalen Resilienz ist, dass die allgemeine wie auch die konkrete Gefährdungslage zumindest im Überblick bekannt sind. Eine regelmäßige Risikobewertung sollte aufgrund der dynamischen Entwicklung im Cyber- und Informationsraum durchgeführt und geeignete präventive sowie reaktive Maßnahmen sollten ausgewählt werden. Szenariobasierte Simulationen von Cyber-Sicherheitsvorfällen können anschließend die Reaktionsfähigkeit und die Robustheit von Sicherheitsmechanismen unter realen Bedingungen erproben.

Fachkräfte

Eine große Herausforderung der Unternehmen ist die Gewinnung von Fachkräften im Bereich der Cyber-Sicherheit aus einer stark umworbenen Zielgruppe. Wirtschaftsführer sehen den Handlungsbedarf eher bei ihren Unternehmen. Externe Dienstleister und die Fortbildung der eigenen Mitarbeiter sind die bevorzugte Quelle für das Know-how im Bereich IT-Sicherheit in den Unternehmen. Führungskräfte können langfristig darauf bauen und anlassbezogen Fachkräfte extern rekrutieren. Unternehmen und Behörden sollten mit Kompetenzzentren und Expertenpools das Fachwissen konzentrieren und anlassbezogen Expertise austauschen.

Industrie 4.0

Die neue Netzinfrastruktur 5G kann Industrie 4.0 neue Schubkraft verleihen. 5G bietet nicht nur mehr Bandbreite, niedrigere Reaktionszeiten, hohe Verfügbarkeit und Qualität in der Datenübertragung; es bringt auch neue Herausforderungen im Hinblick auf die Sicherheit mit sich. Deutlich mehr Führungskräfte haben sich mit dem Thema Industrie 4.0 beschäftigt, aber nur wenige sehen darauf aufbauende Änderungen der eigenen Cyber-Security-Strategie. Das größte Potenzial von 5G liegt in industriellen Anwendungen. Damit es nicht zum größten Risiko des Unternehmens wird, sollten Führungskräfte zumindest neue Risikobewertungen für die relevanten Bereiche durchführen lassen und mögliche Handlungsmaßnahmen ableiten sowie umsetzen.

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.

Stand 11/2019