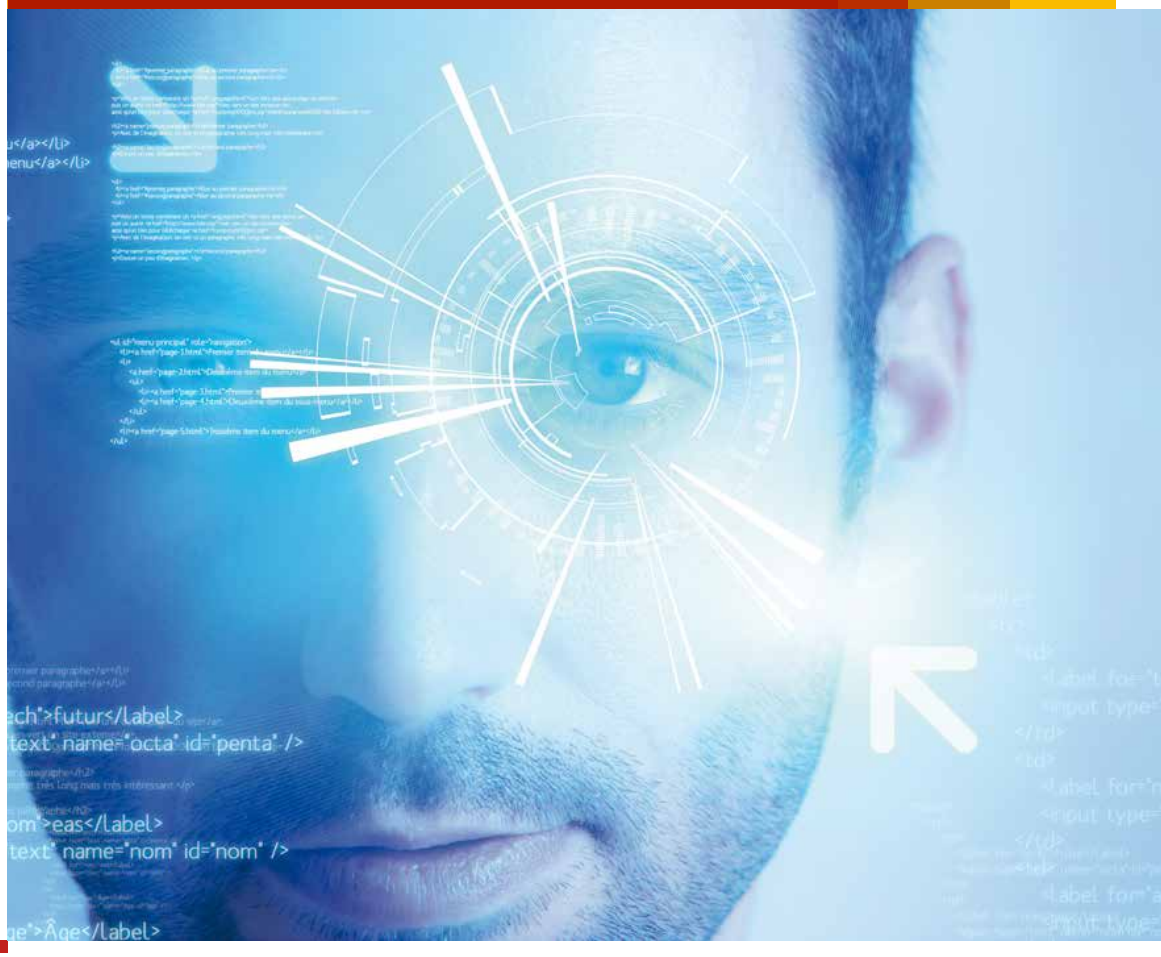
Im Visier der Cyber-Gangster

So gefährdet ist die Informationssicherheit im deutschen Mittelstand

Studie zu Informationssicherheit, Cyberangriffen und -risiken sowie zur Umsetzung des IT-Sicherheitsgesetzes.



pwc

Im Visier der Cyber-Gangster

Herausgegeben von der PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC)

Von Philipp Engemann, Derk Fischer, Björn Gosdzik, Tobias Koller und Nial Moore

Februar 2017, 28 Seiten, 17 Abbildungen, Softcover

Inhaltsverzeichnis

A Einleitung: Im Visier der Cyber-Gangster

Der Druck auf den Mittelstand steigt: Angriffe auf die Unternehmens-IT durch gefälschte E-Mails, eingeschleuste Schadsoftware oder Botnets gehören heute zu den größten Risiken für Unternehmen. Sie legen Produktionslinien lahm, schädigen den Ruf, schrecken die Kunden ab und verursachen somit enormen finanziellen und immateriellen Schaden. Die Angreifer unterscheiden dabei schon lange nicht mehr zwischen Großkonzernen und Mittelstand. Deutsche Familienunternehmen und Mittelständler sind ebenso massiv betroffen, zumal sie oft schlechter gesichert sind als öffentlich bekannte Kapitalgesellschaften. Gleichzeitig setzen sie auf Digitalisierung, transformieren ihre Geschäfts- und Produktionsprozesse, vernetzen sich mit Zulieferern, Geschäftspartnern und Kunden. Dadurch entstehen hochkomplexe IT-Infrastrukturen, die völlig neue Herausforderungen an die Informationssicherheit stellen.

Die Folge: Cyberangriffe nehmen nicht nur zahlenmäßig zu – die Methoden der Angreifer werden zugleich immer aggressiver, ausgefeilter und umfassender. Trotz dieser Bedrohung sind mittelständische Unternehmen bei Investitionen in die Informationssicherheit weiterhin zögerlich und sichern ihre digitalisierten Prozesse und die dafür notwendige IT-Infrastruktur nicht angemessen ab. Dass diese Informationssicherheitsrisiken vielfach ignoriert werden, ist überraschend, vergeht doch kaum ein Tag, an dem nicht über Cyberattacken in der öffentlichen Berichterstattung zu lesen ist.

Etwas risikobewusster und sensibler agieren Unternehmen, die als Betreiber sogenannter Kritischer Infrastrukturen (KRITIS) gelten – allerdings vor allem durch Druck von außen. Denn für sie hat der Gesetzgeber mit dem 2015 in Kraft getretenen IT-Sicherheitsgesetz (IT-SiG) klare Anforderungen an die Informationssicherheit gestellt. Zwar gibt es auch bei ihnen noch Nachholbedarf, der Rückstand ist aber deutlich geringer als bei den meisten anderen mittelständischen Unternehmen. Vielfach unterschätzen letztere nämlich indirekte Auswirkungen des IT-Sicherheitsgesetzes auf das eigene Unternehmen, selbst wenn keine Kritischen Infrastrukturen betrieben werden: Das IT-SiG setzt einen Mindeststandard, an dem sich auch der Mittelstand orientieren sollte, um allgemein akzeptierten Standards zu genügen. Zusätzlicher Druck kommt von EU-Ebene, wo aktuell eine Richtlinie diskutiert wird, die die Anforderungen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen verschärft. EU-weit könnten diese Anforderungen über das deutsche IT-SiG sogar noch hinausgehen und mittelständische Unternehmen zum Handeln zwingen.

In der Neuauflage unserer Studie zum Stand der Informationssicherheit in mittelständischen Unternehmen untersuchen wir, wie gut sich Firmen derzeit gegen Bedrohungen schützen. Zeigt das IT-SiG erste Erfolge? Wie wird sich die Bedrohungslage auch im Hinblick auf die zunehmende Digitalisierung weiterentwickeln? Welche Rolle spielt das Internet der Dinge in diesem Kontext? Lagern Mittelständler die Absicherung der Informationsverarbeitung verstärkt an externe Sicherheitsspezialisten aus? Wie verändert sich das Risikobewusstsein bei Unternehmen, die sich als „Hidden Champions“ vor Angriffen vermeintlich sicher wähnen?

Unternehmen sind mehr denn je gefordert, sich in immer kürzerer Zeit neu zu erfinden und zu verändern. Die Fähigkeit zur digitalen Transformation und die damit einhergehenden Fragen zur Informationssicherheit bilden dabei einen wesentlichen Differenzierungsfaktor. Die Reaktion der Unternehmer auf die neuen Sicherheitsanforderungen entscheidet, ob der Mittelstand insoweit das in ihn gesetzte Vertrauen seiner Geschäftspartner und Kunden verdient und behält.

Dr. Peter Bartels
Vorstandsmitglied und Leiter Familienunternehmen und Mittelstand, PwC

Derk Fischer
Partner für Cyber Security, PwC

B Sicherheit ja – Investitionen nein

1 Das IT-Sicherheitsgesetz

Ende Juli 2015 ist in Deutschland das IT-Sicherheitsgesetz (IT-SiG) in Kraft getreten. Es bündelt eine Vielzahl regulatorischer Vorgaben für die Informationssicherheit in Unternehmen und schreibt damit erstmals bundesweit einheitliche, branchenübergreifende Informationssicherheitsrichtlinien vor. Das IT-SiG ist für Betreiber sogenannter Kritischer Infrastrukturen (KRITIS) bindend.

Zu diesen gehören Unternehmen, die „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden".

Die bereits in Kraft getretene Verordnung zur Bestimmung von Betreibern Kritischer Infrastrukturen berücksichtigt bisher lediglich die Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung. Im Frühjahr 2017 folgt dann die weitere Verordnung für Unternehmen der Sektoren Finanzen, Transport und Verkehr sowie Gesundheit.

Folgerichtig ist die Anzahl der Unternehmen, die nach eigener Einschätzung von dem IT-SiG betroffen sind, 2016 stark gestiegen: 22 % der befragten mittelständische Unternehmen stufen sich als KRITIS-relevant ein; im Vorjahr waren es nur 14 %.

Abb. 1 Betroffenheit durch das IT-SiG

Unternehmen, die sich als Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes einstufen

14 %
*Einschätzung **2015** vor Inkrafttreten des Gesetzes*

22 %
*Einschätzung **2016** nach Inkrafttreten des ersten Gesetzesteils*

Das IT-SiG fordert, dass alle Betreiber Kritischer Infrastrukturen bis 13. Juni 2017 folgende gesetzliche Vorgaben umsetzen:

- einen Informationssicherheitsbeauftragten benennen, der jederzeit für das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Ansprechpartner zur Verfügung steht (inkl. Stellvertreterregelung),
- ein Informations-Sicherheits-Management-System (ISMS) zur Identifikation von Cyberangriffen etablieren, das sich an einem gängigen Standard orientiert, und
- eine Meldestelle einrichten, die das BSI über Cyberangriffe informiert.

Ziel des IT-SiG ist es, die Funktionsfähigkeit und Bedrohungen von IT-Systemen und digitalen Infrastrukturen transparenter zu machen und so vor diesen Gefahren besser zu schützen.

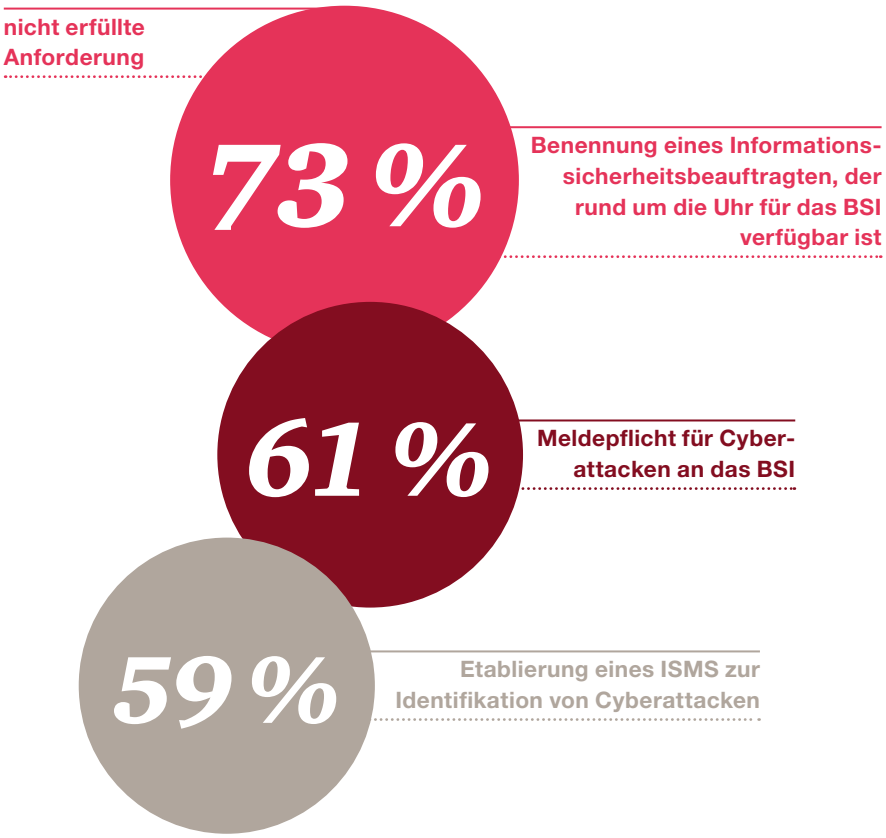
2 Zögerliche Umsetzung der Anforderungen

Doch obwohl das Bewusstsein für die mögliche eigene Betroffenheit gestiegen ist, haben erst wenige Unternehmen daraus Konsequenzen gezogen. Denn sie setzen die Vorschriften des IT-SiG nur zögerlich um.

Nicht einmal die Hälfte der KRITIS-relevanten Unternehmen erfüllte 2016 die Anforderungen des Gesetzes, obwohl die Vorgaben bis Juni 2017 umzusetzen sind:

- 73 % der befragten Unternehmen geben an, bisher keinen Informationssicherheitsbeauftragten als Ansprechpartner für das BSI benannt zu haben.
- Auch die Einrichtung einer Meldestelle für Cyberangriffe steht bei 61 % der befragten Mittelständler noch aus, obwohl die Frist zur Registrierung einer Kontaktstelle beim BSI für die Sektoren Wasser, Energie, Ernährung sowie Informationstechnik und Telekommunikation am 3. November 2016 abgelaufen ist.
- 59 % der Unternehmen haben noch kein Informationssicherheits-Managementsystem (ISMS) implementiert. Das IT-SiG schreibt ein solches System vor, damit Cyberangriffe identifiziert, Abwehrmaßnahmen getroffen und Schwachstellen behoben werden können.

Unternehmen aus dem öffentlichen Sektor scheinen besser aufgestellt zu sein. 35 % geben dort an, sowohl einen Informationssicherheitsbeauftragten benannt zu haben als auch der Meldepflicht für Cyberattacken an das BSI nachkommen zu können. Lediglich bei der Etablierung eines ISMS sind diese mit 53 % etwas schlechter aufgestellt.



3 Wer Sicherheit will, muss investieren

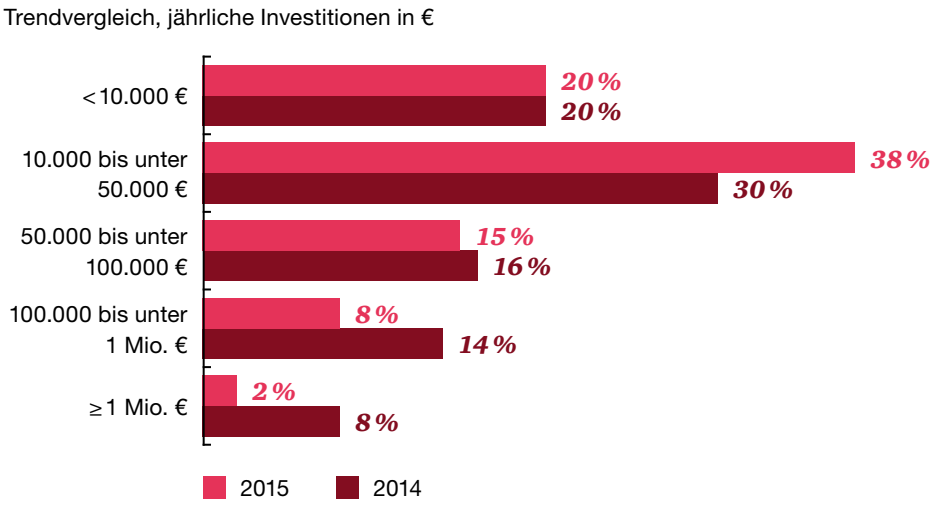
Weder das IT-SiG noch die erhöhte Gefahr durch Cyberangriffe konnten bisher die Investitionen in Informationssicherheit ankurbeln. Im Gegenteil: Die IT-Budgets der mittelständischen Unternehmen sind im Vergleich zur Vorjahresstudie sogar gesunken. Investitionen zwischen 100.000 bis unter 1 Million Euro schrumpften von 14 % auf 8 %. Ausgaben über 1 Million Euro sind im Bereich Informationssicherheit nach wie vor die Ausnahme.

Doch nur durch fortwährende Anpassungen und Investitionen kann sich der Mittelstand gegen immer neue Formen und Arten von Cyberangriffen wappnen. Werden dagegen heute notwendige Investitionen vertagt, steigen die Risiken und sehr oft die daraus entstehenden Folgekosten. Ein Grund für die dennoch zurückhaltende Investitionstätigkeit der Unternehmen ist möglicherweise die mangelnde Planungssicherheit: Denn bisher hat der Gesetzgeber im Rahmen des IT-SiG nur einzelne Sektoren als Betreiber Kritischer Infrastrukturen bestimmt.

„Das IT-Sicherheitsgesetz ist ein Rahmengesetz, das neben dem Schutz sogenannter Kritischer Infrastrukturen darauf abzielt, die Informationssicherheitssysteme auf Unternehmensseite generell zu verbessern. Die Gefahrenlage durch Cyberattacken hat sich derart verschärft, dass sich auch Betreiber nicht kritischer Infrastrukturen mit dem IT-SiG aktiv auseinandersetzen und mehr in Informationssicherheit investieren müssen. Das IT-SiG wird sich als Standard etablieren und dabei auch als unternehmensinterne Argumentationshilfe für mehr Investitionen in Informationssicherheit dienen.“

Derk Fischer, Partner für Cyber Security, PwC.

Abb. 2 Investitionen der befragten Unternehmen in Informationssicherheit



Der öffentliche Sektor ist mit Investitionen besonders zurückhaltend. 62 % investierten weniger als 50.000 Euro; lediglich ein Bruchteil (6 %) gab mehr als 100.000 Euro für die Informationssicherheit aus.

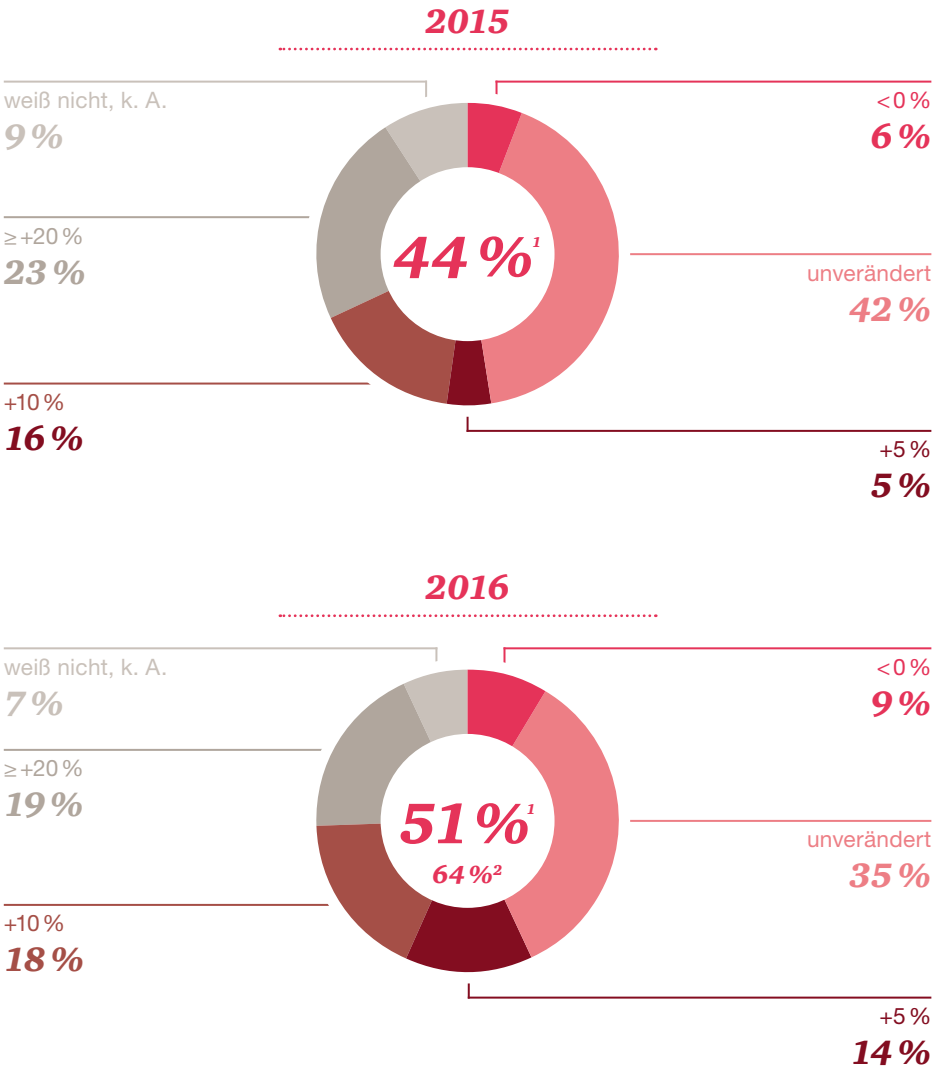
4 Investitionsentwicklung

Die erwartete Entwicklung der zukünftigen Investitionen lässt aber auf einen steigenden Stellenwert der Informationssicherheit schließen: 2016 hielten 51 % eine positive Ausgabenentwicklung im Bereich der Informationssicherheit für wahrscheinlich, 2015 waren es 44 %. KRITIS-Unternehmen schätzen sich 2016 (Vergleichszahl 2015 liegt nicht vor) dabei als weitaus investitionsfreudiger ein. Fast zwei Drittel – nämlich 64 % – gehen von einer deutlichen Erhöhung der Budgets für Informationssicherheit aus.

Ob diesen Einschätzungen Taten folgen werden, ist ungewiss. Bereits im Vorjahr erwarteten 39 % der Befragten einen Investitionsanstieg von mehr als 10 %, 2015 wurde dann aber deutlich weniger investiert als im Vorjahr.

Abb. 3 Einschätzung der Entwicklung der Investitionen in Informationssicherheit

Trendvergleich „Wie schätzen Sie die Entwicklung der Investitionen für Informationssicherheit für 2016 ungefähr ein?“



[1] Anteil jener Unternehmen, die im aktuellen Jahr steigende Investitionen erwarten.
[2] Anteil der KRITIS-Unternehmen.

5 Druckpunkt „Digitale Transformation“

Treiber der steigenden Investitionen in Informationssicherheit sind vor allem äußere Faktoren. Zum einen zwingen regulatorische Anforderungen zu mehr Aktivität: 46 % der vom IT-SiG betroffenen Unternehmen wollen aus diesem Grund ihre Investitionen um mehr als 10 % erhöhen. Bei Unternehmen, die sich nicht vom IT-SiG betroffen fühlen, liegt dieser Anteil nur bei 33 %. Zum anderen kommt Druck von externen Stakeholdern, etwa Kunden oder Geschäftspartnern: 66 % der Mittelständler geben Kundenanforderungen als Grund für Investitionen in die Informationssicherheit an.

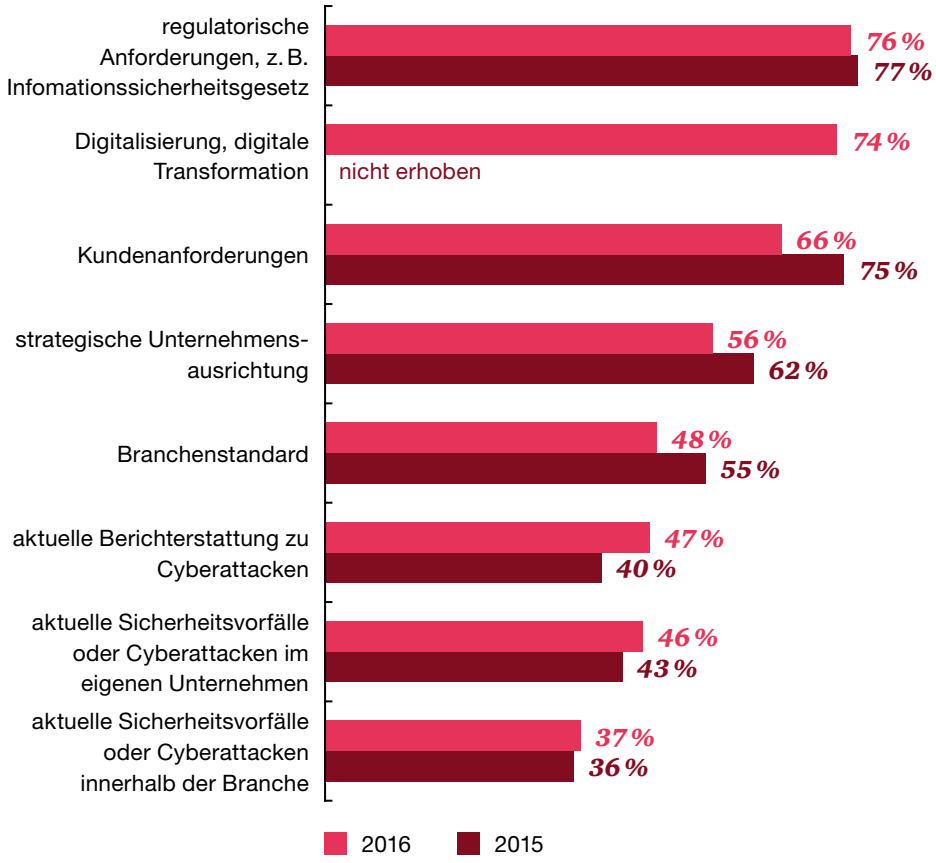
Auch die zunehmende digitale Transformation diverser Branchen, insbesondere im Zuge von Industrie 4.0, macht zukünftig höhere Investitionen erforderlich (vgl. Kapitel E). Durch die voranschreitende inner- und überbetriebliche Vernetzung verschwimmen die klassischen Grenzen der Informationssicherheit und es entstehen zahlreiche neue Schnittstellen und Prozesse im erweiterten Bereich der Cyber Security. Neben dem Schutz sensibler Unternehmens- und Kundendaten wird eine hohe Verfügbarkeit der zugrunde liegenden IT-Systeme immer wichtiger.

Unternehmen müssen nicht länger nur ihre eigenen Informationen und informationsverarbeitenden Systeme, sondern umfassende Wertschöpfungsketten schützen, die vielfach global organisiert sind.

Ganze Branchen sind gefordert, ganzheitliche Sicherheitskonzepte zu entwickeln – über Unternehmensgrenzen bzw. verteilte Wertschöpfungsketten hinweg.

Abb. 4 Gründe, in Informationssicherheit zu investieren

Trendvergleich „Warum wird Ihr Unternehmen in den nächsten Jahren in Informationssicherheit investieren?“



Risiken dezentraler Wertschöpfungsketten am Beispiel der Automobilindustrie

In der Automobilindustrie spielen Zulieferer eine wichtige Rolle. Die Sicherheit dieser Schnittstelle entlang der Wertschöpfungskette ist wichtig und spiegelt sich in einem zweiseitigen Prozess wider: Zum einen haben die Automobilhersteller ein großes Interesse daran, sensible Produktinformationen, Patente oder auch Projektplanungen zu schützen. Diese Absicherung wälzen sie auf ihre Partner ab und fordern von ihnen einen modernen Sicherheitsmanagementprozess. Auf der anderen Seite nutzen viele Zulieferer genau dieses Argument, um sich von ihren Wettbewerbern abzusetzen. Neben der dadurch entstehenden Positionierung als sicherer Partner greifen auch Argumente wie Kosten- und Zeitminimierung. Zulieferer sind darauf angewiesen, termingerecht zu arbeiten. Durch die Integration eindeutig definierter Sicherheitsprozesse profitieren sie von weniger Sicherheitsvorfällen, sparen Kosten ein und verkürzen Lieferzeiten.

„Daten sind das Herz eines Unternehmens“
Derk Fischer, Partner für Cyber Security, PwC, im Interview

Welche Sicherheitsbedrohungen sind Ihrer Meinung nach besonders akut?
Durch die zunehmende Digitalisierung vergrößern sich die Angriffsvektoren für Cyberattacken; völlig neue Bedrohungsszenarien entstehen. Erpressungen via Ransomware und Cryptolocker sowie CEO-Fraud, auch Chef-Trick genannt, sind das Thema schlechthin. Darüber hinaus haben Firmen mit großflächigen „Distributed Denial of Service (DDoS)“-Angriffen zu kämpfen, die die Verfügbarkeit ihrer Dienste einschränken. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt, dass auch der Anteil an Schadsoftware im E-Mail-Verkehr deutlich zugenommen hat.

Zum Trendthema Ransomware: Wie genau funktioniert sie und wieso ist sie so gefährlich für den Mittelstand?
Für jedes Unternehmen sind die eigenen Daten zu Kunden, Aufträgen und Produkten das Herz ihrer Geschäftstätigkeit. Im Gegensatz zu Konzernen sichern mittelständische Unternehmen ihre Daten häufig in längeren Zeitintervallen, sodass das letzte Backup nicht immer den aktuellsten Stand hat. Weiterhin ist es mittelständischen Unternehmen oft nicht möglich, die Datensicherungen in einem abgeschotteten Netzwerksegment abzulegen. Hier kommt Ransomware ins Spiel, ein zusammengezogener Begriff aus Ransom – Englisch für Lösegeld – sowie Software, die die Hacker nutzen, um die Unternehmen zu erpressen. Öffnet ein Mitarbeiter einen vermeintlich harmlosen E-Mailanhang, verschlüsselt das angehängte Programm die lokale Festplatte oder verbreitet sich im Netzwerk des betroffenen Unternehmens. Sofern keine ausreichende Sicherung vorhanden ist, muss der Unternehmer auf die Forderung des Erpressers eingehen, um wieder an seine Daten zu gelangen.

Angenommen ein Unternehmen hat seine Hausaufgaben im Bereich Backups gemacht. Ist es dann sicher vor Erpressung?
Leider nein. Gerade Onlinehändler und Internetdienstleister sind Zielscheibe der sogenannten DDoS-Erpressung. Bei einer solchen Attacke versucht der Angreifer, die Verfügbarkeit eines Dienstes durch sehr viele Anfragen bzw. Datenpakete zu beeinträchtigen oder zum Erliegen zu bringen. Bei dem betroffenen Unternehmen können große Umsatzeinbußen entstehen, wenn etwa ein Onlineshop nicht mehr erreichbar ist. Der Hacker verschickt im Vorfeld des Angriffs ein Erpresserschreiben an das Unternehmen und kündigt einen DDoS-Angriff für den Fall an, wenn kein Lösegeld gezahlt wird. Häufig verleihen die Erpresser der Forderung Nachdruck, indem sie einen kurzen Angriff durchführen und die eigene Leistungsfähigkeit demonstrieren. Möglich werden DDoS-Angriffe durch Botnetze, die für Unternehmen ein weiteres Sicherheitsrisiko bilden.

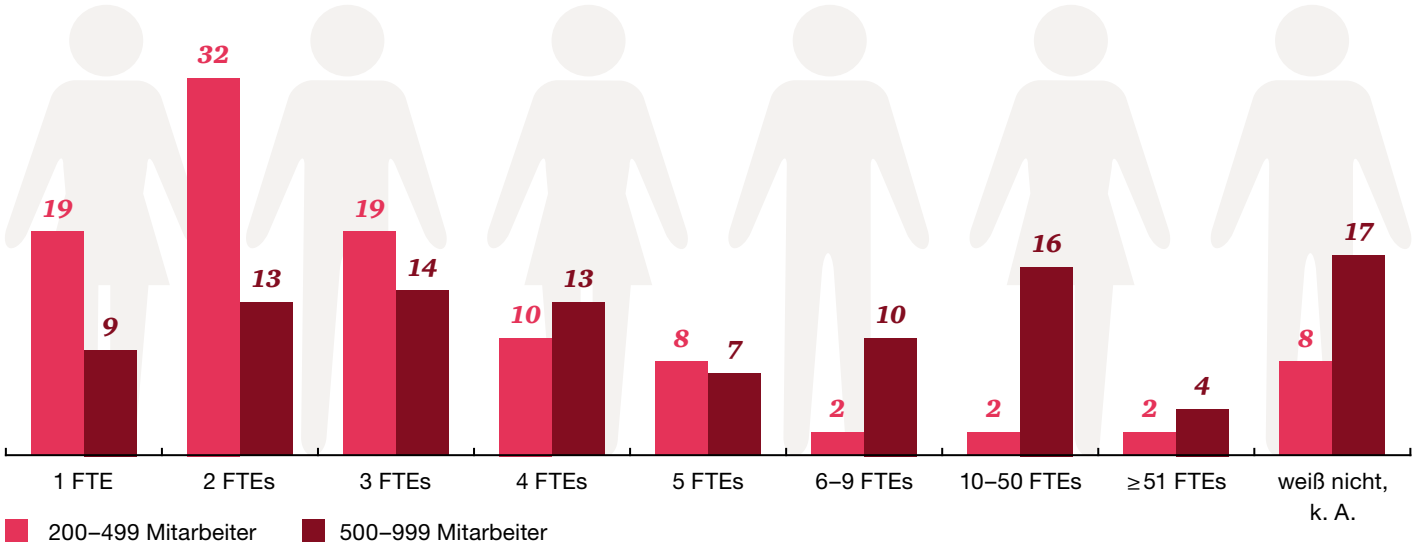
Welche Gefahren entstehen Unternehmen durch Botnetze?
Ein Botnetz (in Anlehnung an den robot) ist ein Verbund von Computern, mobilen Geräten und zunehmend auch internetfähigen Geräten, die von einer Schadsoftware befallen sind und so von außen gesteuert werden können. Prinzipiell kann jedes internetfähige Gerät Teil eines Botnetzes werden. Hacker nutzen sie vor allem, um IT-Systeme durch DDoS-Attacken anzugreifen, oder zum Versenden von Spam und Schadsoftware. Durch die Verbindung von sehr vielen Geräten über das Internet bieten Botnetze den Kriminellen eine hohe Rechnerkapazität und Bandbreite, die sie für Angriffe nutzen können.

6 Personalausstattung – mangelhaft?

Die erwartete Ausgabenentwicklung zeigt bisher jedoch keinen Effekt auf die Personalausstattung: Die Anzahl der Mitarbeiter, die mit der Informationssicherheit betraut sind, bleibt im Vergleich zum Vorjahr konstant: Bei 36 % der Unternehmen sind unverändert nur ein bis zwei Mitarbeiter (Full Time Equivalents, FTEs) für Informationssicherheit verantwortlich. Die Unternehmensgröße spielt dabei eine wesentliche Rolle. Während entsprechende Aufgaben bei Unternehmen bis 500 Mitarbeiter mehrheitlich (51 %) von maximal zwei FTEs bewältigt werden, sind bei Unternehmen mit mehr als 500 Mitarbeitern drei FTEs und mehr keine Seltenheit (64 %).

Ein Grund dafür liegt sicherlich im Fachkräftemangel. 2016 fehlten in Deutschland laut Bitkom[1] 51.000 IT-Spezialisten – vom Softwareentwickler über Digitalexperten bis hin zum Informationssicherheitsspezialisten. Und die offenen Stellen sind gegenüber dem Vorjahr um 20 % gestiegen. Denkbar ist aber auch die fehlende Einsicht, Sicherheitsrisiken durch personelle Ressourcen auffangen zu müssen.

Abb. 5 Anzahl der in der Informationssicherheit tätigen Mitarbeiter in Prozent



[1] Vgl. www.bitkom.org/Presse/Presseinformation/51000-offene-Stellen-fuer-IT-Spezialisten.html.

7 Informationssicherheit ist Chefsache

Ein positives Signal ist jedoch das gestiegene Bewusstsein der Unternehmenschefs für die Wichtigkeit von Informationssicherheit: Neun von zehn Beauftragten für Informationssicherheit (88 %) berichten an die Geschäftsführung – damit ist die Informationssicherheit im deutschen Mittelstand in erster Linie Chefsache.

„Der Mittelstand hat zweifellos noch Luft nach oben, was seine Investitionen sowohl finanzieller als auch personeller Art in die Informationssicherheit angeht. Regulatorische Vorgaben wie das IT-SiG erzeugen sicherlich Druck. Viel wichtiger aber ist, dass die Unternehmen selbst aktiv werden und aus eigener Motivation heraus entsprechende Sicherheitsstrukturen aufbauen.“

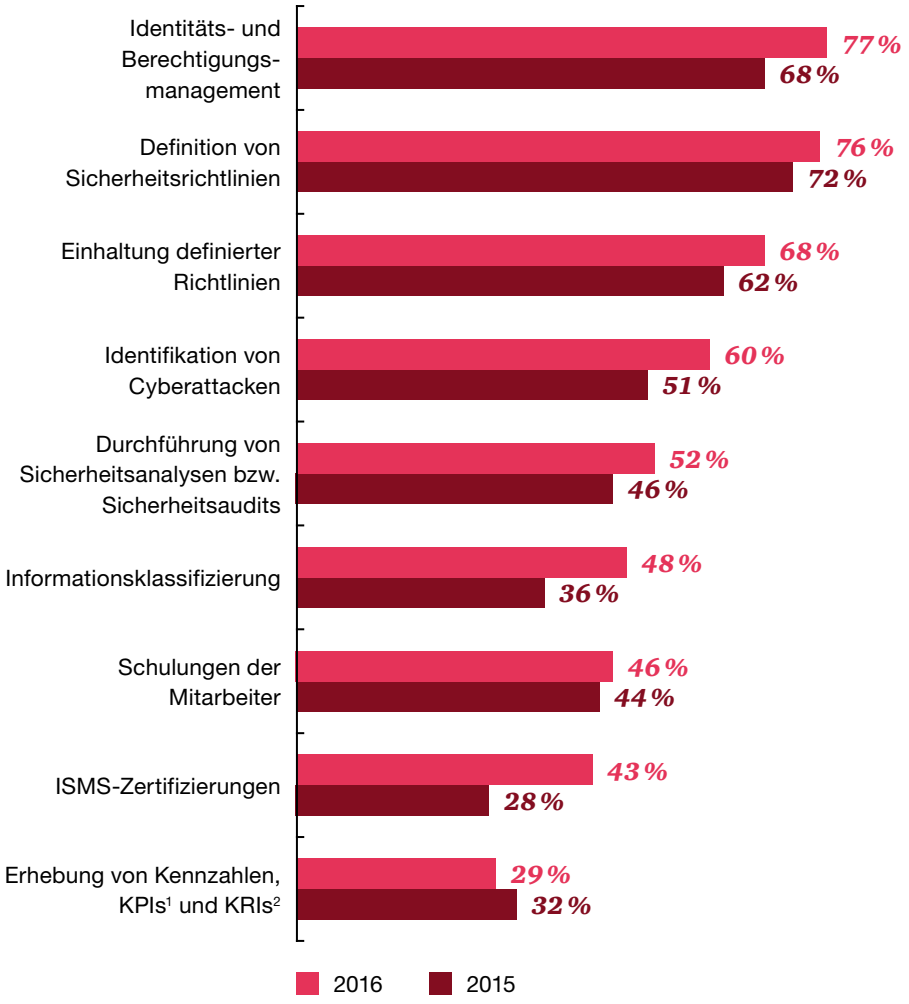
Derk Fischer, Partner für Cyber Security, PwC.

8 Selbsteinschätzung vs. Umsetzung

Trotz der zögerlichen Umsetzung des IT-SiG und (bisher) geringen IT-Budgets fühlt sich die Mehrheit (72 %) der 400 befragten Privatunternehmen gut oder sehr gut gegen Cyberattacken geschützt. Gleichzeitig lässt sich bei der Bewertung der Umsetzung verschiedener Informationssicherheitsprozesse generell ein positiver Trend beobachten: So fühlen sich Unternehmen im Identitäts- und Berechtigungsmanagement sowie in der Definition und Einhaltung von Sicherheitsrichtlinien deutlich besser aufgestellt als im Vorjahr. Nachholbedarf gibt es dagegen bei der Erhebung von Key-Performance-Indikatoren (KPIs) und Key-Risk-Indikatoren (KRIs). Nicht einmal ein Drittel der Unternehmen schätzt diesen Bereich im eigenen Unternehmen als „gut“ oder „sehr gut umgesetzt“ ein.

Abb. 6 Bewertung des Informationssicherheitsprozesses

Trendvergleich „gute“ oder „sehr gute“ Umsetzung



[1] KPI: Key-Performance-Indikator
[2] KRI: Key-Risk-Indikator

C Informationssicherheit bleibt interne Aufgabe

Heutige Cyberangriffe sind derart ausgefeilt, dass ihre Abwehr ein hohes Maß an Know-how und Ressourcen erfordert. Für Unternehmen gilt es, IT-Prozesse, -Systeme und -Infrastrukturen mit Blick auf die neuesten Angriffsarten, Schwachstellen und Schutzmaßnahmen ständig auf dem aktuellen Stand zu halten. Das schließt auch regelmäßige Schulungen der eigenen Mitarbeiter ein. Gerade die IT-Abteilungen mittelständischer Unternehmen können dies aber aus personellen, zeitlichen und budgetären Gründen oft nicht leisten und sind daher in vielen Fällen nicht ausreichend gegen mögliche Angriffsszenarien gewappnet.

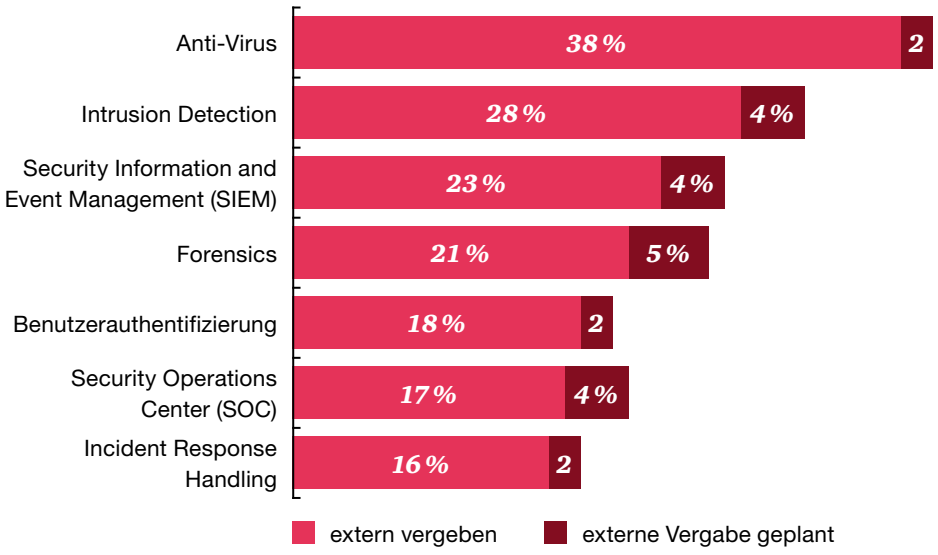
Vor diesem Hintergrund kann die Auslagerung von Sicherheitsaufgaben an externe Dienstleister mehrere Vorteile haben. Bei sorgfältiger Auswahl des Anbieters (Managed Services Providers, MSP) finden die Unternehmen dort das entsprechende Know-how und können sich auf ihr Kerngeschäft konzentrieren. Darüber hinaus können externe Dienstleister, anders als die Unternehmen selbst, spezialisiertes Personal häufig in sehr kurzer Zeit aufstocken, etwa wenn dies bei laufenden Cyberangriffen notwendig werden sollte.

Die aktuelle Befragung zeigt allerdings, dass der Großteil der Informationssicherheitsaufgaben im deutschen Mittelstand immer noch von eigenen Mitarbeitern durchgeführt wird. Auch in naher Zukunft wollen viele Unternehmen die Zusammenarbeit mit externen Sicherheitsspezialisten kaum ausbauen. Selbst bei Spezialthemen wie Intrusion Detection (systematische Entdeckung von Angriffen) und Security Information and Event Management (SIEM) gibt es nur geringe Zuwächse bei der Bereitschaft, Externe mit dem Aufbau und Betrieb solcher Lösungen zu beauftragen.

Dabei wird verkannt, dass externe Expertise eine effektive Verbesserung der eigenen Sicherheitssituation darstellt. So bewerten beispielsweise Unternehmen, die externe Unterstützung beim Incident Response Handling in Anspruch nehmen, ihren Schutz vor Cyberangriffen als besser als diejenigen, die dies nicht tun. Auch haben sie mehr Vertrauen in den Prozess der Identifikation und Behandlung von Angriffen auf das Unternehmen.

Abb. 7 Externe Sicherheitsdienstleistungen

Welche der folgenden Dienstleistungen sind in Ihrem Unternehmen extern beauftragt?



Was sich gut auslagern lässt

Anti-Virus: *Anti-Virus-Programme für Systeme, beispielsweise Server oder Workstations*

Intrusion Detection: *System zum systematischen Entdecken von Angriffen durch Monitoring von Netzwerkverkehr*

Security Information and Event Management (SIEM): *System zum Erkennen und Behandeln sicherheitsrelevanter Ereignisse, zum Beispiel bei Endgeräten, Servern und Netzwerkgeräten*

Forensics: *Untersuchung von Angriffen und Verdachtsfällen und Sicherung gerichtsverwertbarer Dokumentationen*

Benutzerauthentifizierung: *Management von Identitäten und Authentifizierung von Benutzern über die (gesamte) System- und Anwendungslandschaft, zum Beispiel durch zentrale Systemlösungen*

Security Operations Center (SOC): *Kompetenzeinheit zur Sicherung und Verbesserung der Fähigkeiten zur Bekämpfung und Prävention von Cyberbedrohungen*

Incident Response Handling: *strukturierter Umgang mit den Folgen eines Angriffs oder Security Breach*

D Zielscheibe Mittelstand

1 Entwicklung der Bedrohungslage

Das aktuelle Stimmungsbild zeigt: Für einen Großteil – nämlich zwei Drittel – der befragten mittelständischen Unternehmen hat sich die Bedrohungslage durch Angriffe auf die Informationstechnik verschärft. Ein besonders hohes Gefahrenpotenzial sehen vor allem Unternehmen der Kritischen Infrastruktur und hier in erster Linie die Branchen Gesundheitswesen, Energie und Technologie.

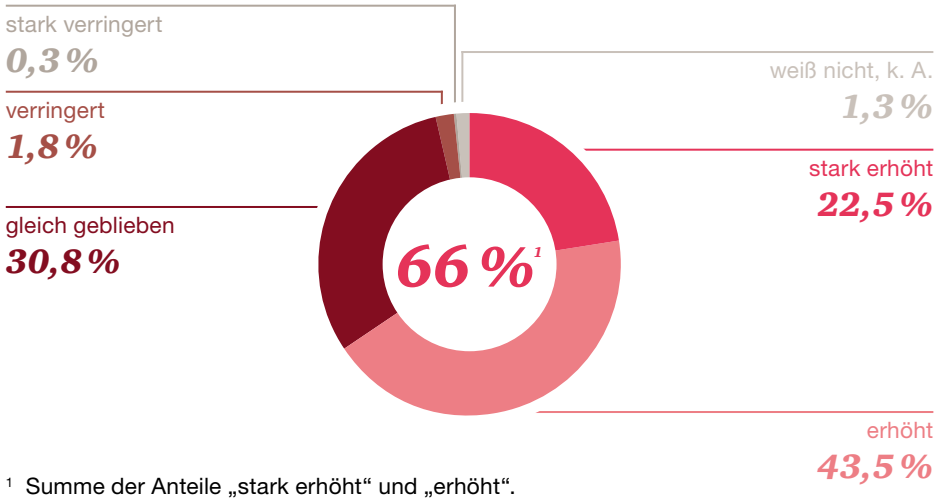
Bemerkbar macht sich die verschärfte Lage vor allem durch neue Angriffsarten (Ransomware, CEO-Fraud, Internet der Dinge, Botnetz), eine erhöhte Zahl von Angriffen auf die Unternehmen, aber auch durch die verstärkten Aktivitäten auf Gesetzgeberseite, zum Beispiel mit zusätzlichen gesetzlichen Vorgaben wie dem IT-Sicherheitsgesetz.

Trotzdem stufen mehr als ein Drittel (37 %) der Unternehmen, welche die Bedrohungslage für erhöht oder stark erhöht halten, ihre Prozesse zur Identifikation von Cyberangriffen als höchstens durchschnittlich ein. 11 % gaben sogar an, dass der Prozess zur Erfassung von Cyberangriffen in ihrem Unternehmen unzureichend implementiert ist. Ihre Aktivitäten in der Sicherheitsanalyse der eigenen IT-Landschaft halten 14 % der Unternehmen für unterdurchschnittlich.

Dies zeigt, dass sich viele mittelständische Unternehmen noch immer so gut vor Cyberangriffen geschützt fühlen, dass sie auf die Verbesserung der eigenen Sicherheitsprozesse und -maßnahmen verzichten. Die Schere zwischen der allgemein wahrgenommenen Bedrohungslage und dem Bewusstsein für das eigene Risiko klafft somit noch stark auseinander.

Abb. 8 Entwicklung der Bedrohungslage

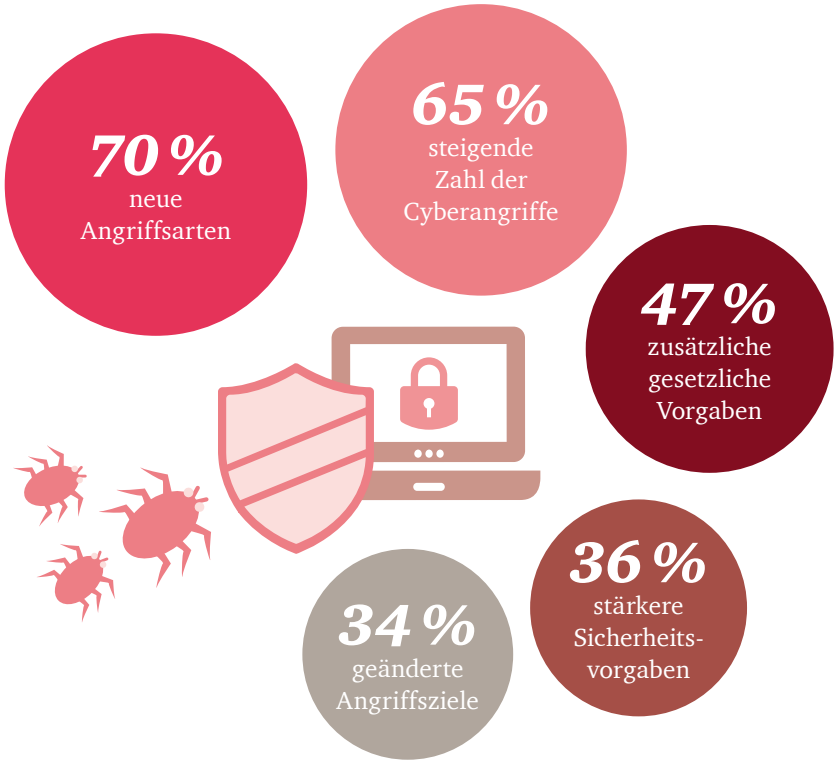
„Wie hat sich die Bedrohungslage durch Cyberangriffe in den letzten 12 Monaten aus Ihrer Sicht geändert?“



[1] Summe der Anteile „stark erhöht“ und „erhöht“.

Abb. 9 Falls erhöht: Auswirkungen

„Wie macht sich die erhöhte Bedrohungslage für Ihr Unternehmen bemerkbar?“



2 Verdopplung der Anzahl der Angriffe

Das gestiegene Bewusstsein für eine verschärfte Bedrohungslage durch Cyberangriffe entspricht auch den Tatsachen: Die Zahl von Angriffen auf die eigene IT-Landschaft ist gestiegen. Nahezu jedes fünfte privatwirtschaftliche Unternehmen gibt an, in den letzten zwölf Monaten von mindestens einem erfolgreichen Cyberangriff betroffen gewesen zu sein. Im Vorjahr war es nur jedes zehnte Unternehmen. Damit hat sich die Anzahl der Unternehmen, die erfolgreich angegriffen wurden, innerhalb eines Jahres fast verdoppelt.

Verwunderlich ist das nicht – denn der deutsche Wirtschaftsraum mit seinen innovativen technik-, produkt- und ingenieurgetriebenen mittelständischen Unternehmen ist für Angreifer ein attraktives Ziel. Neue und noch nicht abgesicherte Schnittstellen an den Prozessübergängen sind mögliche Einfallstore für Bedrohungen wie Erpressertrojaner, die Ausspähung von Zugangsdaten oder großflächige DDoS-Attacken.

„Es gibt noch viele mittelständische Unternehmen, die ihre IT für ausreichend halten. Als „Hidden Champions“ unterliegen sie dem Irrglauben, dass ihr Bekanntheitsgrad nicht so hoch ist und sie damit weniger im Visier von Cyberkriminellen sind. Aber gerade sie sind hochinnovativ und deshalb leider auch oft hochattraktiv, wenn es zum Beispiel um den Diebstahl geistigen Eigentums geht.“

Dr. Peter Bartels, Vorstandsmitglied und Leiter Familienunternehmen und Mittelstand, PwC.

Abb. 10 Von erfolgreichen Cyberangriffen betroffene Unternehmen

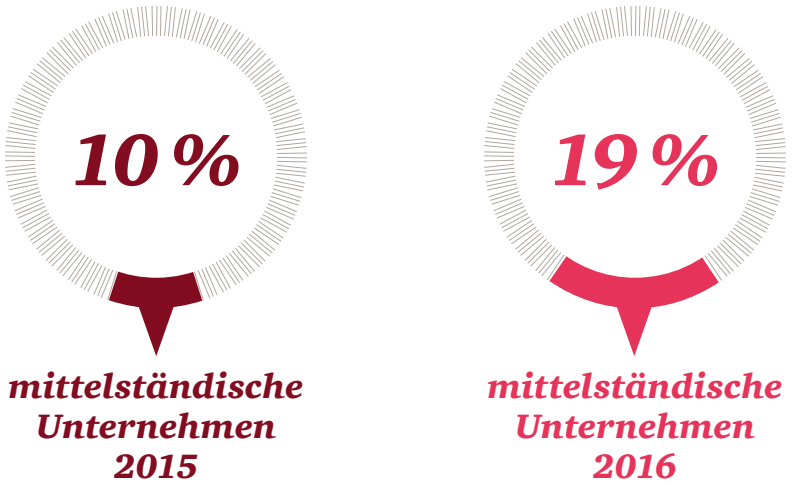
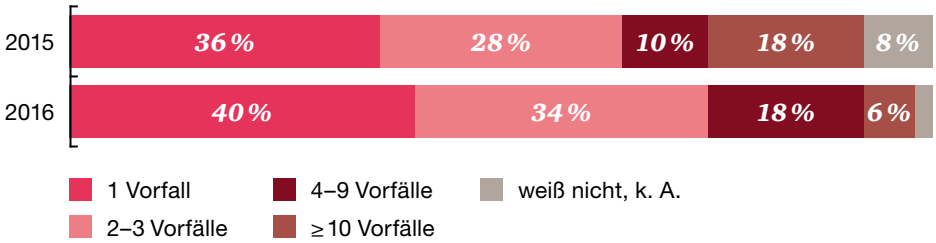


Abb. 11 Betroffene Unternehmen: Anzahl der Vorfälle



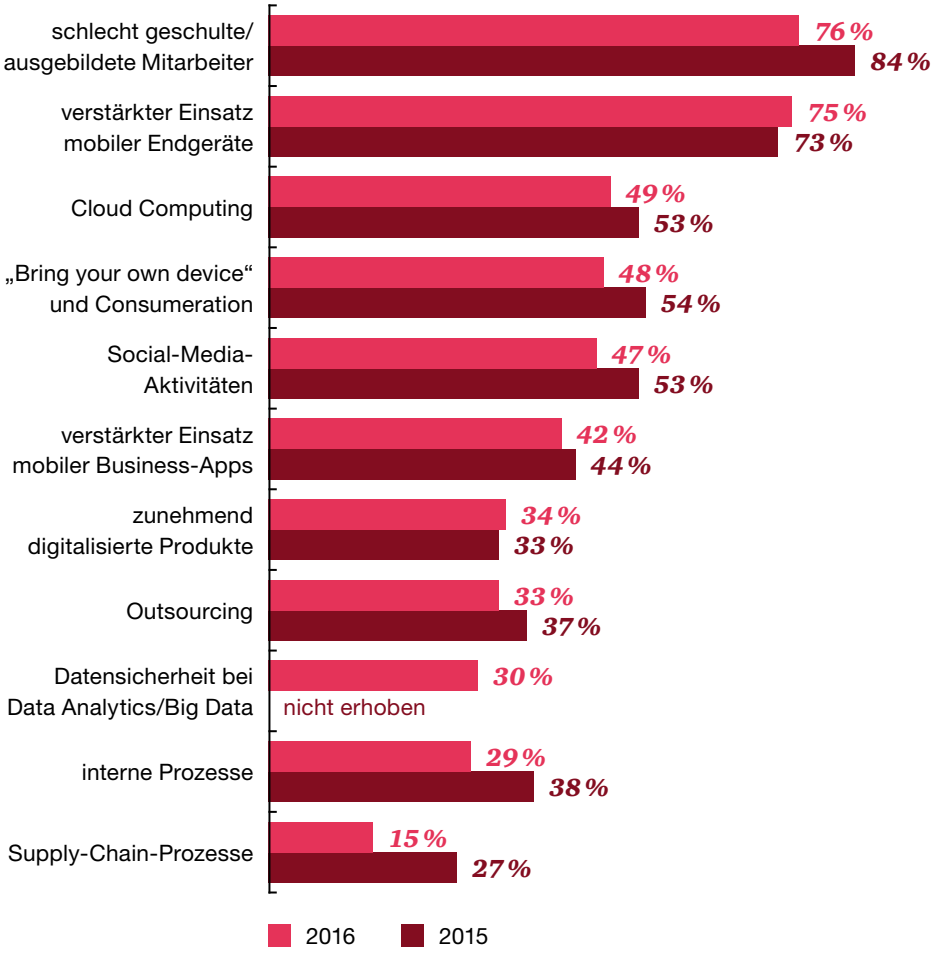
3 Die Risikofaktoren

Als größte Gefahrenquelle wird – wie auch im Vorjahr – der Faktor Mensch angesehen. Für 76 % der Befragten sind schlecht geschulte bzw. ausgebildete Mitarbeiter ein hohes Sicherheitsrisiko – und das über alle Branchen und Unternehmensgrößen hinweg.

Als weitere nennenswerte Risikofaktoren gelten die zunehmende Nutzung mobiler Endgeräte, Cloud Computing, „Bring your own device", Social-Media-Aktivitäten der Unternehmen sowie der verstärkte Einsatz mobiler Business-Apps.

Abb. 12 Worin Unternehmen Sicherheitsrisiken sehen

Trendvergleich „Welche der folgenden Entwicklungen bringen Ihrer Meinung nach die größten Sicherheitsrisiken für das Unternehmen mit sich?"



„Mensch versus Maschine“

Dr. Peter Bartels, Vorstandsmitglied und Leiter Familienunternehmen und Mittelstand, PwC, im Gespräch

Welche Rolle spielt bei der Informationssicherheit eigentlich der Mensch?
Eine Sicherheitsstrategie kann nur so gut sein wie ihre Umsetzung durch die Mitarbeiter im Unternehmen. Auch bei aktueller und störungsfreier IT ist der Mensch ein Risikofaktor, der gerne vergessen wird. Für Angreifer ist er die einfachste „Schwachstelle“, um in ein Netzwerk von außen einzudringen. Die meisten Angriffe durch Phishing, Spam oder sogenanntes Social Engineering setzen am Benutzer an. Deswegen ist es so wichtig für Unternehmen, die eigenen Mitarbeiter für die Methoden von Kriminellen zu sensibilisieren und ein Bewusstsein für sicherheitsveranwortliches Handeln im Alltag zu schaffen.

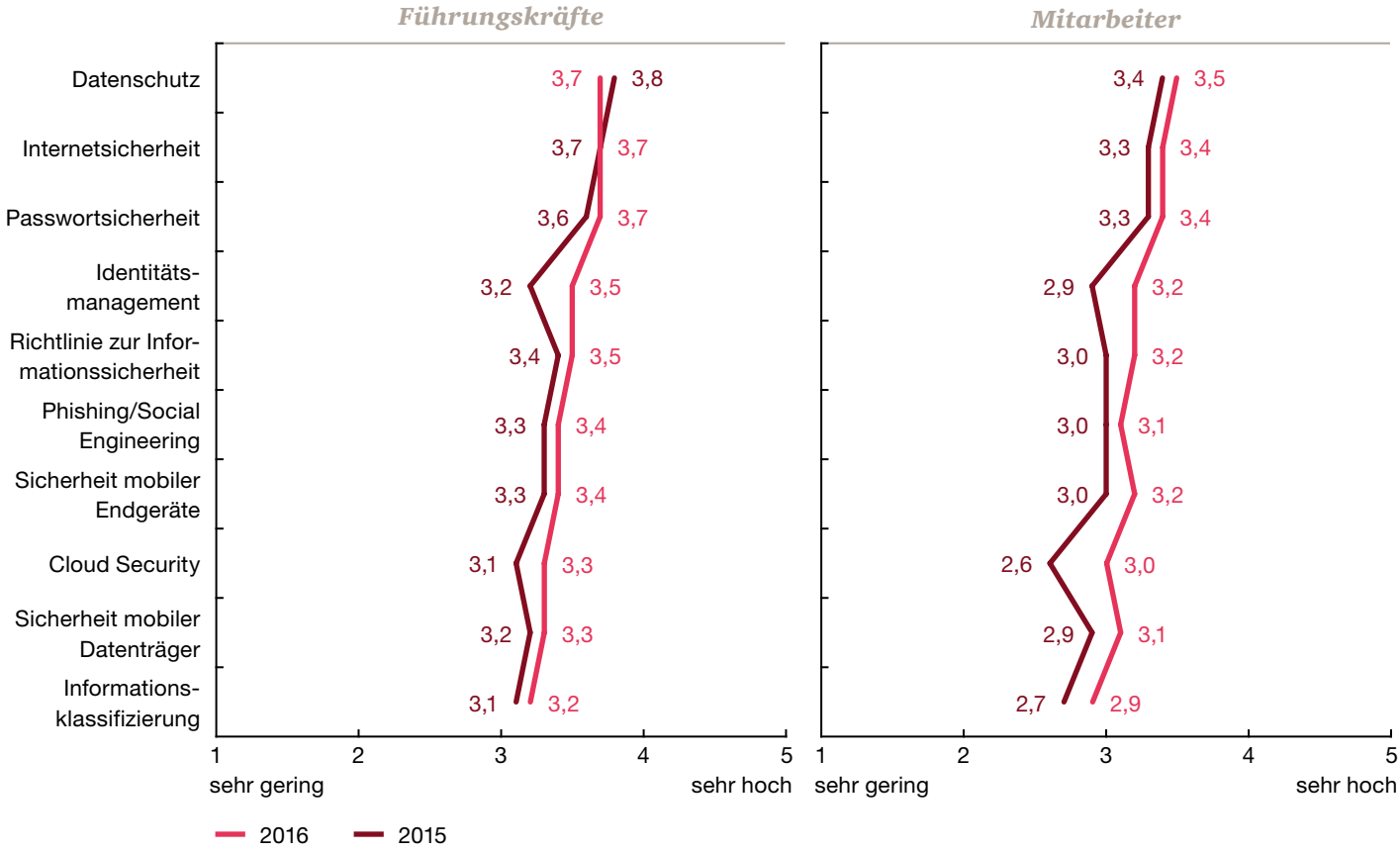
Die neuen Trends lassen erkennen, dass sich die IT immer stärker automatisiert und in Zukunft sogar mit Künstlicher Intelligenz (KI) zu rechnen ist. Löst das das Problem menschlicher Risiken?
Im Gegenteil, mit der Durchdringung der IT mit vernetzten und autonomen Systemen stellen sich ganz neue Fragen in Bezug auf die Informationssicherheit. Richtig ist, dass Maschinen im direkten Vergleich zu Menschen unbestechlich und daher für Angriffe durch Spam oder Social Engineering nicht empfänglich sind. Allerdings entstehen durch automatisierte Systeme immer komplexere Anwendungen, die häufig auch von Menschen nicht mehr vollständig durchschaut werden. Sind diese Systeme dann von außen zugänglich, besteht die Gefahr, dass diese durch das Vorspiegeln falscher Daten kompromittiert werden oder als Einfallstor für weitere Angriffe über das Netzwerk dienen.

Mit der Entwicklung fortgeschrittener Künstlicher Intelligenz und selbst lernender Systeme ergeben sich in Zukunft also wieder neue Sicherheitsfragen?
Absolut – vor allem im Hinblick auf die Entscheidungsautonomie dieser Maschinen, die Auswirkungen auf die Informationssicherheit von innen haben. Ein Beispiel sind Algorithmen, die an den Börsen im Millisekundentakt Entscheidungen treffen. Technische Fehler können hier zu Kettenreaktionen führen, die für Menschen erst sehr spät zu erkennen sind. Hier gilt es, die an Maschinen übertragene Handlungsautonomie gegen die vertretbaren Risiken abzuwägen und abzusichern.

Konsequenzen ziehen daraus nur wenige Unternehmen. Geschult wird zwar zu gängigen Themen wie dem korrekten Umgang mit und dem Schutz von Kundendaten, Datenschutz, Meldung von Informationssicherheitsvorfällen und zur Internetsicherheit. Es hapert aber noch an Trainings zum richtigen Umgang mit mobilen Endgeräten und Awareness-Schulungen zu den Themen Phishing und Social Engineering. Im Bereich Cloud Computing sehen nur 23 % der Unternehmen ihre Mitarbeiter als ausreichend sensibilisiert an, doch lediglich 15 % der Unternehmen bieten entsprechende Schulungen an.

Abb. 13 Sensibilisierung für Themen der Informationssicherheit

Grad der Sensibilisierung (Durchschnittswerte)
„Wie schätzen Sie die Sensibilisierung der Mitarbeiter für die folgenden Bereiche der Informationssicherheit ein?“



4 Die Ziele der Cyberkriminellen

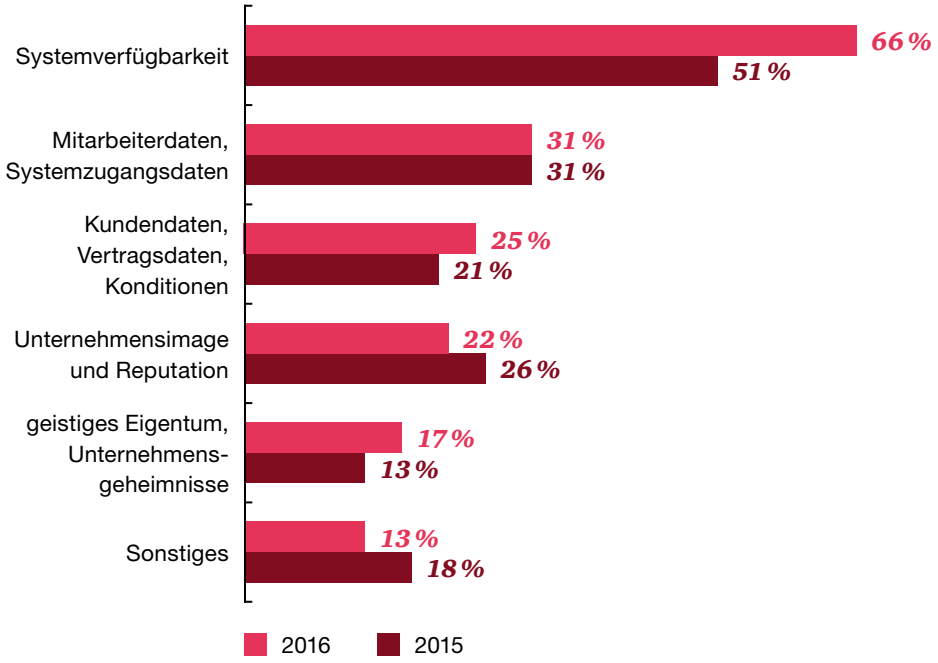
66 % der befragten Unternehmer geben als häufigstes Ziel der Angreifer die Beeinträchtigung der Systemverfügbarkeit an. Das ist wenig überraschend, denn bei zunehmend vernetzten Wertschöpfungsketten zwischen Unternehmen, Lieferanten und Kunden spielt eine durchgängige und gleichbleibende Systemverfügbarkeit eine zentrale Rolle. Fallen Systeme wiederholt aus oder sind beeinträchtigt, kommt es zu teils gravierenden Störungen im gesamten Betriebsablauf. Bei Betreibern Kritischer Infrastrukturen nannten sogar 82 % die Systemverfügbarkeit als Angriffsziel.

Mitarbeiter- und Systemzugangsdaten sind ein weiteres begehrtes Angriffsziel. Sie öffnen Tür und Tor für kriminelle Aktivitäten wie Datendiebstahl und Cyberspionage. Im Jahr 2016 lag der Anteil der Unternehmen, die Angriffe auf Mitarbeiterdaten und Systemzugänge gemeldet hat, auf dem Niveau des Vorjahres. Für Angreifer sind besonders Firmen aus dem produzierenden Gewerbe interessant – mit 45 % rangieren sie deutlich über dem Durchschnittswert von 31 %.

Bei jedem vierten Mittelständler haben es die Angreifer auch auf Kunden- und Vertragsdaten abgesehen. Mit einem Anstieg von 21 % auf 25 % gegenüber dem Vorjahr ist hier eine leichte Verschärfung zu beobachten. Rückläufig sind in der Wahrnehmung der Unternehmen die Attacken, die darauf abzielen, Image und Reputation eines Unternehmens negativ zu beeinflussen. Sie sanken von 26 % auf 22 %.

Abb. 14 Angriffsziele

Trendvergleich „Was waren die primären Ziele der Angreifer?“

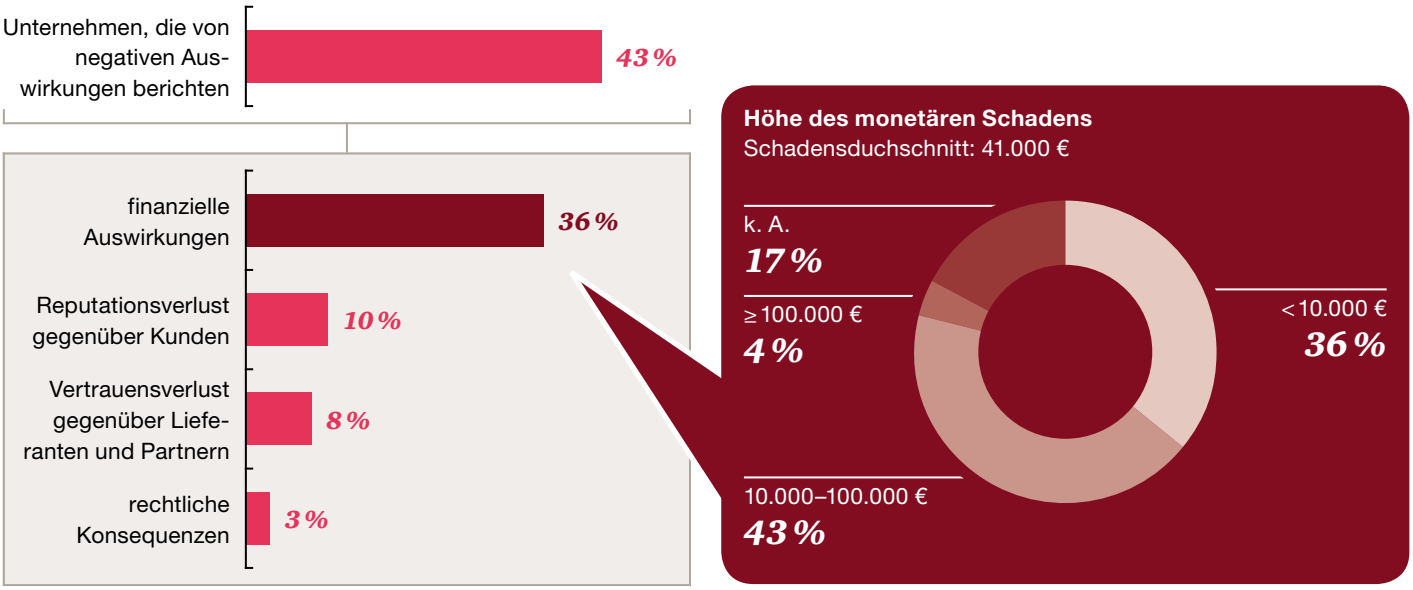


5 Finanzieller Schaden oft nicht bekannt

Ein ramponiertes Image oder eine schlechte Reputation zu beziffern, ist schwierig, und generell lassen sich die finanziellen Auswirkungen durch Cyberattacken nicht immer genau benennen.

So war jedes fünfte befragte Unternehmen, das in den vergangenen zwölf Monaten Opfer eines erfolgreichen Cyberangriffs war, nicht in der Lage, eine Angabe über die Höhe des monetären Schadens zu machen. Das wird oft dadurch erschwert, dass nicht nur ein einzelnes System (z. B. eine produzierenden Maschine) für einen bestimmten Zeitraum ausfällt, sondern gesamte Netzwerke lahmgelegt werden. Zudem sind häufig mehrere Abteilungen mit ihren Mitarbeitern oder gar das gesamte Unternehmen betroffen.
Ein dritter beeinflussender Faktor ist, dass oft nicht alle erfolgreichen Cyberangriffe entdeckt werden, was die Schätzung der Gesamtschäden durch Cyberangriffe zusätzlich erschwert. Sinnvoll ist deshalb die Entwicklung aussagekräftiger Kennzahlen, mit denen der Nutzen der Investitionen – also die vermiedenen monetären Schäden – beziffert werden kann. Denn so können Kosten und Nutzen am wirkungsvollsten gegeneinander abgewogen werden.

Abb. 15 Negative Auswirkungen auf betroffene Unternehmen

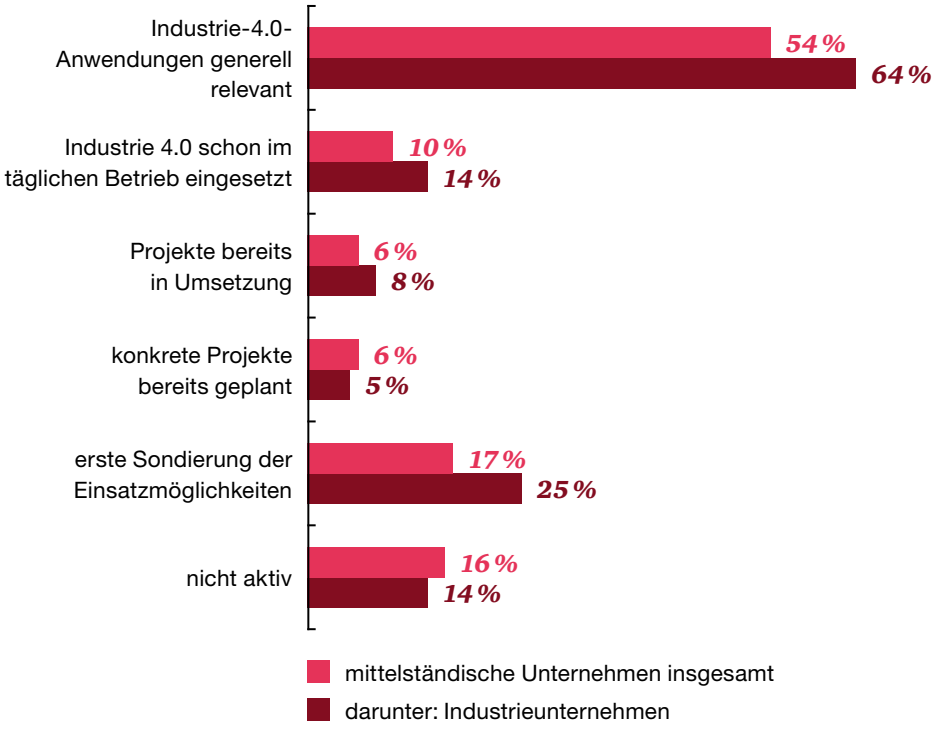


E Industrie 4.0: Angriff auf die digitale Wertschöpfungskette

Leistungsfähigere IT-Systeme halten verstärkt Einzug in Organisationen und treiben die Digitalisierung und Automatisierung von Geschäftsprozessen voran. Die Smart Factory ist längst kein Zukunftsszenario mehr: Bis 2020 werden über 80 % der Unternehmen ihre Wertschöpfungskette digitalisiert haben.[2] Auch bei mittelständischen Unternehmen ist die digitale Aufbruchstimmung spürbar: So ist für mehr als die Hälfte (54 %) von ihnen das Thema Industrie 4.0 relevant. 17 % sondieren noch Einsatzmöglichkeiten, 12 % planen konkrete Projekte oder setzen diese bereits um, und immerhin jedes zehnte Unternehmen nutzt Industrie-4.0-Anwendungen bereits im täglichen Betrieb. In Industrieunternehmen sind diese Anteile noch einmal deutlich höher.

Abb. 16 Cyber Security im Rahmen von Industrie 4.0

In wieweit ist Ihr Unternehmen schon im Bereich Industrie 4.0 aktiv?



[2] Vgl. PwC, Industrie 4.0 – Chancen und Herausforderungen der vierten industriellen Revolution, 2014.

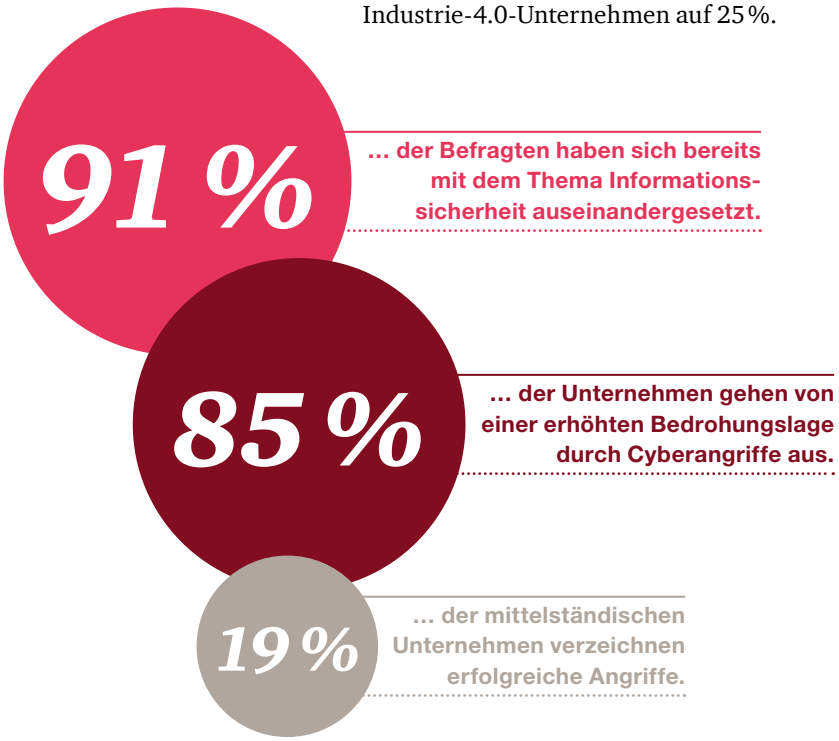
Die zunehmende Vernetzung interner und externer Bereiche (beispielsweise Produktion und Verwaltung mit externen Lieferanten) sowie die Erweiterung bisheriger Produkte um digitale Kundenservices bringen eine höhere Anfälligkeit für verschiedene Angriffsszenarien mit sich. So erlaubt beispielsweise eine Internetanbindung von Industrieanlagen, diese per Fernwartung zu überwachen und Störungen schnell zu beheben. Diesem Vorteil steht jedoch ein erhöhtes IT-Risiko gegenüber. Denn durch gezielte Manipulation lassen sich ganze Produktionslinien lahmlegen, etwa indem Thermostate oder Füllstandsanzeigen falsche Werte anzeigen und daraufhin eine fehlerhafte Steuerung erfolgt.

Dass Unternehmen mit Industrie-4.0-Aktivitäten anfälliger sind und häufiger zur Zielscheibe von Cyberangriffen werden, zeigt sich auch in den Befragungsergebnissen: Während insgesamt jedes fünfte mittelständische Unternehmen (19 %) erfolgreiche Angriffe auf seine Strukturen verzeichnete, stieg dieser Anteil bei Industrie-4.0-Unternehmen auf 25 %.

Zudem berichten Unternehmen mit vernetzter Produktion überdurchschnittlich häufig von einer Zunahme der Cyberbedrohungen: 85 % von ihnen gehen von einer erhöhten oder sogar stark erhöhten Bedrohungslage durch Cyberangriffe in den letzten zwölf Monaten aus (mittelständische Unternehmen insgesamt: 66 %).

Dass Industrie-4.0-Aktivitäten ein erhöhtes Sicherheitsrisiko darstellen, ist den meisten Unternehmen bewusst. Sie wissen, dass für die Zuverlässigkeit von Industrie-4.0-Anwendungen und -Systemen sowie den Schutz sensibler Unternehmensdaten ein hohes Maß an Informationssicherheit notwendig ist. So haben sich bereits 91 % der befragten Verantwortlichen mit dem Thema Informationssicherheit bei der Umsetzung ihrer Industrie-4.0-Tätigkeiten auseinandergesetzt.

Dieses Bewusstsein spiegelt sich auch in den getätigten sowie geplanten Investitionen in Informationssicherheit wider. So haben mittelständische Unternehmen, die Industrie 4.0 bereits im täglichen Betrieb verwenden, in der Vergangenheit durchschnittlich höhere Investitionen in Informationssicherheit getätigt und erwarten auch eine höhere Investitionsbereitschaft als die Unternehmen, für die Industrie 4.0 aktuell keine Bedeutung hat. Ob die Investitionen in Art und Umfang allerdings ausreichend sind, bleibt abzuwarten.



F Zusammenfassung

Mittelständische Unternehmen werden immer häufiger Zielscheibe von Cyberangriffen, und das Gros der befragten Unternehmen ist sich dessen auch bewusst. Das gestiegene Bewusstsein für eine erhöhte Gefährdungslage entspricht dabei der tatsächlichen Lage: So zeigen die Studienergebnisse eine Verdopplung der Angriffe, die immer aggressiver, ausgefeilter und umfassender werden. Den Cyberkriminellen geht es meist um die Beeinträchtigung der Systemverfügbarkeit, die im Hinblick auf die zunehmend vernetzten Wertschöpfungsketten zwischen Unternehmen, Lieferanten und Kunden ein zentraler Erfolgsfaktor ist.

Der Mittelstand ist immer häufiger im Visier von Cyber-Gangstern und ist sich dessen auch bewusst. Hauptziel der Kriminellen ist die Beeinträchtigung der Systemverfügbarkeit.

Wie im Vorjahr gilt der Faktor Mensch über alle befragten Branchen und Unternehmensgrößen hinweg als größtes Sicherheitsrisiko. Mitarbeiter sind in Fragen der Informationssicherheit noch zu wenig geschult und ausgebildet. Konsequenzen ziehen daraus aber nur wenige Firmen und fokussieren sich weiterhin auf gängige Schulungsthemen.

Der Faktor Mensch ist weiterhin das größte Sicherheitsrisiko.

Trotz des massiven Anstiegs von Attacken auf den deutschen Mittelstand und trotz des zunehmenden Bewusstseins, mehr in Informationssicherheit investieren zu müssen, reagieren die Firmen nur zögerlich mit konkreten Maßnahmen. Dennoch schätzen sich die Unternehmen in Bezug auf die eigene Sicherheit als gut oder sehr gut geschützt ein. Damit klaffen Selbsteinschätzung und tatsächliche Bedrohungslage auseinander. Die Erfahrung zeigt, dass Angriffe in vielen Fällen gar nicht erst erkannt werden, was zu einem trügerischen Sicherheitsgefühl beiträgt. Hinzu kommt: Oft kennen betroffene Unternehmen die Höhe der finanziellen Schäden nicht genau, da Cyberattacken zu spät erkannt und bewertet werden. Das lässt viele Unternehmen schlussfolgern, dass sich teure Investitionen in die Informationssicherheit nicht lohnen.

Trotz der Bedrohungslage reagieren die betroffenen Firmen nicht bzw. nur unzureichend mit konkreten Maßnahmen in Richtung erhöhter IT-Budgets und -Ressourcen.

Dass Betreiber Kritischer Infrastrukturen (KRITIS) sich besser gegen Cyberattacken schützen, ist eine Folge des 2015 in Kraft getretenen IT-Sicherheitsgesetzes. Sie haben den Druck von Gesetzgeberseite, effektive Sicherheitsmanagementsysteme unternehmensintern aufzubauen. Aber auch hier gelingt dies nur schwerfällig. Nicht einmal die Hälfte der KRITIS-relevanten Unternehmen hat die Gesetzesanforderungen bislang umgesetzt, die bis Juni 2017 zu erfüllen sind.

Es zeichnet sich kein Sicherheitsruck ab, auch nicht bei den als KRITIS eingestuften Unternehmen.

Auch wenn viele Mittelständler zu wenig in die Informationssicherheit investieren, so erwarten die Unternehmen dennoch einen leichten Aufwärtstrend bei zukünftigen Investitionen. Zudem zeigt sich, dass das Thema in den Chefetagen für immer wichtiger erachtet wird.

Leichter Investitionsanstieg wird erwartet, Chefetagen nehmen Informationssicherheit ernster.

Obwohl die mittelständischen Unternehmen die Dringlichkeit moderner Informationssicherheitsstrukturen erkannt haben, sind es nicht die Unternehmen selbst, sondern vielmehr äußere Faktoren wie das IT-SiG oder stärkere Sicherheitsanforderungen externer Stakeholder wie Kunden oder Geschäftspartner, die die Firmen antreiben. Auch der digitale Wandel mit voranschreitender inner- und überbetrieblicher Vernetzung erhöht den Druck auf Firmenseite, Schnittstellen und Prozesse zu schützen, um die Systemverfügbarkeit zu gewährleisten und die eigenen Daten zu schützen.

Äußere Faktoren stoßen Investitionen in die Informationssicherheit in den Firmen an. Die Firmen selbst sind noch nicht die Treiber.

G Handlungsempfehlungen

Was bedeuten die Ergebnisse unserer Studie nun für den deutschen Mittelstand, der weiterhin erfolgreich im deutschen und internationalen Wirtschaftsraum agieren möchte? Dass er seine Unternehmensstrukturen besser schützen muss – und zwar durch eine tragfähige und umsetzungsorientierte Informationssicherheitsstrategie.

1. Setzen Sie die Vorgaben des IT-Sicherheitsgesetzes um – nicht nur als Betreiber einer Kritischen Infrastruktur. Die Vorgaben sind ein Mindeststandard, den jedes mittelständische Unternehmen erfüllen sollte.

2. Analysieren Sie, wie gut Sie im Bereich Informationssicherheit schon aufgestellt sind – und wo es Schwachstellen gibt (Maturity Assessment).

3. Ermitteln Sie, wie hoch der Schutzbedarf für Ihre Prozesse, Daten, Informationen und Infrastruktur ist (Business Impact Analysis). Dies hilft Ihnen, die Auswirkungen der Digitalisierung auf Ihr Geschäftsmodell und damit auch Ihre IT-Landschaft abzuschätzen.

4. Erstellen Sie Ihr Risikoprofil, indem Sie verschiedene Risikoszenarien entwickeln und diese priorisieren.

5. Betrachten Sie nicht nur den Istzustand, sondern beziehen Sie künftige Entwicklungen mit IT-Relevanz in Ihre Überlegungen ein.

6. Leiten Sie daraus eine Informationssicherheitsstrategie ab und entwickeln Sie ein Informationssicherheits-Managementsystem (ISMS).

7. Etablieren Sie permanente und automatisierte interne Kontrollprozesse, um Schwachstellen bei der Informationssicherheit schnell, umfassend und dauerhaft zu erkennen und zu bekämpfen. Bedenken Sie, dass dafür nicht nur technische Lösungen notwendig sind.

8. Investieren Sie in Ihre IT-Abteilung, aber auch in alle Ihre Mitarbeiter, vor allem hinsichtlich Schulungen und Qualifizierungen.

H Methodik und Grundlagen der Studie

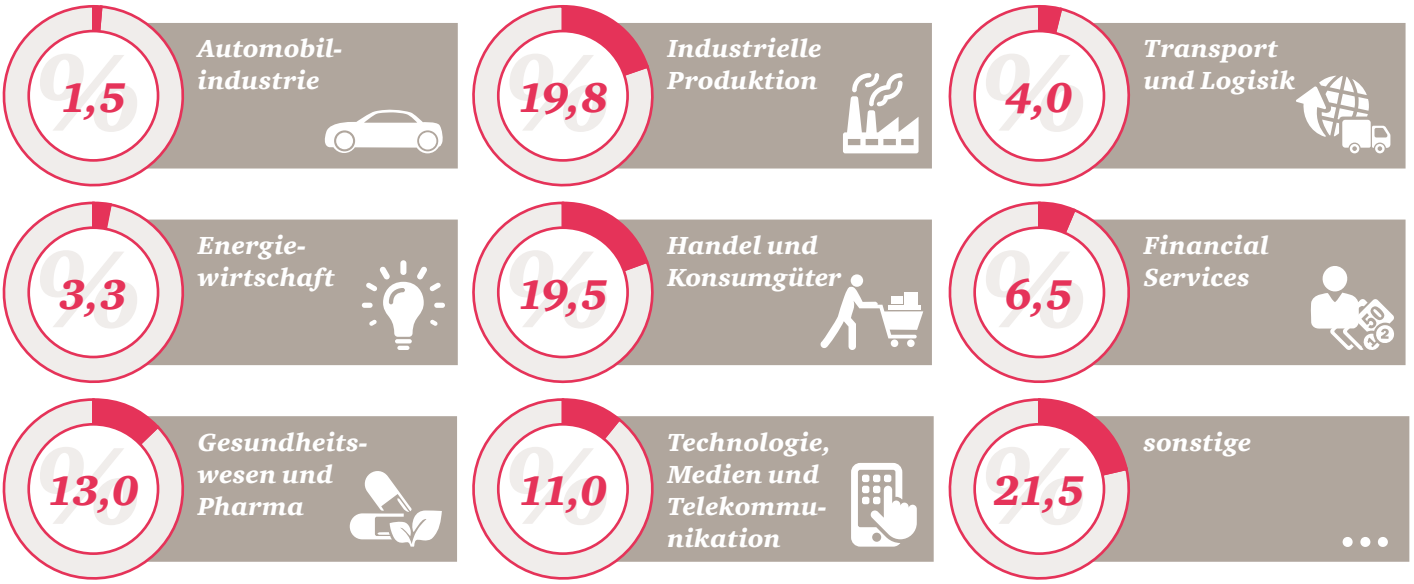
Die vorliegende Studie untersucht den Stand der Informationssicherheit in deutschen mittelständischen Unternehmen im Jahr 2016. Grundlage der Ergebnisse ist eine bundesweite Befragung in Form von computergestützten Telefoninterviews (CATIs) auf Basis eines vollstrukturierten Fragebogens, die durch ein unabhängiges Marktforschungsinstitut im Auftrag von PwC durchgeführt wurde. Im Zeitraum vom 12. September bis zum 28. Oktober 2016 wurden 400 Mittelständler interviewt.

Die Hälfte der befragten Unternehmen des Privatsektors beschäftigt zwischen 200 und 500 Mitarbeiter, weitere 200 Firmen zählen zwischen 500 und 1.000 Angestellte. Damit weichen wir von gängigen Definitionen des Mittelstands ab, die Unternehmen bis zu einer Größe von 250 Mitarbeitern umfassen. Dieses Vorgehen wurde bewusst gewählt, da auch größere mittelständisch geprägte und eigentümergeführte Unternehmen hinsichtlich der Informationssicherheit vergleichbare Strukturen aufweisen.

Auskunft gaben in erster Linie Unternehmensmitarbeiter mit IT-Verantwortung wie IT-Direktoren, Informationssicherheitsmanager und Datenschutzbeauftragte. Vereinzelt wurden auch CEOs und CFOs befragt.

Sämtliche Vergleiche zum Vorjahr beziehen sich auf die Vorgängerstudie Angriff aus dem Cyberspace: So gefährdet sind mittelständische Unternehmen, erschienen im Dezember 2015. Auf Basis derselben Methodik wurden seinerzeit ebenfalls 400 deutsche Mittelständler zum Stand der Informationssicherheit befragt. Inhaltlich erweitert wurde die vorliegende Studie um die Bereiche Security-as-a-Service (SaaS), (Kapitel C) und Industrie 4.0 (Kapitel E). Erstmals befragt wurden außerdem 100 Unternehmen der öffentlichen Hand – aufgrund der fehlenden Vergleichbarkeit zum Vorjahr werden diese Ergebnisse allerdings nicht umfassend dargestellt.

Abb. 17 Aufteilung der Befragten nach Branchen in Prozent



Ihre Ansprechpartner

Dr. Peter Bartels
Vorstandsmitglied und Leiter Familienunternehmen und Mittelstand, PwC
Tel.: +49 211 981-2176
peter.bartels@de.pwc.com

Derk Fischer
Partner für Cyber Security, PwC
Tel.: +49 211 981-2192
derk.fischer@de.pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 157 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

Mittelständische und familiengeführte Unternehmen und deren Inhaber erhalten bei uns eine Betreuung, die sich durch Engagement und Kontinuität auszeichnet. Unseren Mandanten steht ein persönlicher Ansprechpartner zur Seite, den sie jederzeit zu allen Fragen konsultieren können. Er kennt ihr Geschäft, hat die Interessen der Gesellschafter im Blick und koordiniert die Arbeit der jeweils erforderlichen Fach- und Branchenexperten. So bekommen sie alle Leistungen aus einer Hand, zeitnah und direkt vor Ort – auch im Ausland.

PwC. Mehr als 10.300 engagierte Menschen an 22 Standorten. 1,9 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland. Partner für Familienunternehmen und Mittelstand.