Angriff aus dem Cyber Space: So gefährdet sind mittelständische Unternehmen

Die Ergebnisse unserer aktuellen Befragung von 400 mittelständischen Unternehmen in Deutschland.

pwc

Angriff aus dem Cyber Space: So gefährdet sind mittelständische Unternehmen

Die Ergebnisse unserer aktuellen Befragung von 400 mittelständischen Unternehmen in Deutschland.

pwc

Angriff aus dem Cyber Space: So gefährdet sind mittelständische Unternehmen

Herausgegeben von der PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC)

Von Derk Fischer, Dr. Johannes Barnickel, Christian Fuchs, Philipp Engemann, Dr. Björn Gosdzik und Nial Moore

Dezember 2015, 28 Seiten, 12 Abbildungen, Softcover

Inhaltsverzeichnis

Abbildungsverzeichnis

A Einleitung

Digital unterstützte oder gar gesteuerte Lieferketten vom Lieferanten bis hin zum Kunden[1] sind heute in allen Branchen nicht mehr wegzudenken. Auch unternehmensinterne Prozesse werden zunehmend elektronisch abgebildet, sei es im Bereich der Rechnungslegung oder bei der Kommunikation. Mitarbeiter- und Kundendaten werden schon längst digital verwaltet. Dies ermöglicht ein effektives und effizientes Arbeiten, bringt zugleich aber auch Gefahren für das Unternehmen mit sich. Eine der größten Gefahren sind Cyberangriffe, also Angriffe auf die IT-Systeme und Netzwerke eines Unternehmens über das Internet. Die Medien berichten in diesem Zusammenhang immer wieder über gestohlene Unternehmensdaten, manipulierte Netzwerke oder den Zusammenbruch von IT-Systemen.

Seit unserer im März 2014 erschienenen Vorjahresstudie zur IT-Sicherheit haben entsprechende Sicherheitsvorfälle in Deutschland immer wieder für Schlagzeilen gesorgt. Dazu zählen die mit Phishing-Software infizierten Rechner des Deutschen Bundestags ebenso wie die Veröffentlichung von Kundendaten namhafter Konzerne. Doch auch kleine und mittelgroße Betriebe in Deutschland sind vor solchen Angriffen nicht sicher – denn auch sie verfügen über Daten und Informationen, die für potenzielle Angreifer wertvoll sind.

Manchmal ist es hilfreich, sich in die Gegenseite hineinzudenken, um sich ein Problem vor Augen zu führen – beim Thema Informationssicherheit also in den unbekannten Hacker, der irgendwo auf der Welt an einem Computer sitzt und sich von dort aus beliebig in fremde Firmennetze einklinken kann. Was sind seine Motive? Hier ein Ausschnitt aus einem Internet-Chat mit einem Hacker, den wir hier unter dem Pseudonym „Hackermann“ zu Wort kommen lassen.

[1] Der besseren Verständlichkeit und Lesefreundlichkeit halber wird nachfolgend im Text nur die männliche Form der Personenbezeichnung verwendet, gemeint sind selbstverständlich beide Geschlechter.

Interview

Herr Hackermann, warum dringen Sie in Systeme fremder Unternehmen ein?

Hackermann: Neben der technischen Faszination kann man damit gut Geld verdienen. Es gibt einen Schwarzmarkt für persönliche Daten, angefangen von E-Mail-Adressen über Kreditkartendaten bis zu Sozialversicherungsnummern. Und dann natürlich die internen Unternehmensdaten selbst. Dazu ist allerdings mehr Vorbereitung nötig und man muss wissen, wem man diese Daten anbieten kann. So könnte zum Beispiel ein Wettbewerber an neuen Entwicklungen der Konkurrenz interessiert sein.

Interessieren Sie sich eher für große oder kleine Unternehmen?

Hackermann: Große Unternehmen haben zwar mehr Daten gespeichert, aber kleine Firmen sind oft schlecht gesichert. Ich habe oft den Eindruck, die IT-Sicherheit macht da jemand nur so nebenbei, der eigentlich ganz andere Aufgaben hat. Für Hacker ist das leicht verdientes Geld. Da kann man teilweise sogar noch mit automatisierten Tools Erfolg haben. Dann ist es vom Zeitaufwand her fast egal, ob man eine Firma angreift oder 500. So kommen große Mengen an Kundendaten zusammen. Und auch die kleinen Unternehmen haben durchaus lohnende Firmendaten.

Hat sich für Sie in den vergangenen zwölf Monaten etwas verändert?

Hackermann: Es werden immer mehr verschiedenartige Geräte mit dem Internet verbunden, bewusst oder unbewusst. Neben Servern, Arbeitsplatzrechnern und Smartphones sind das zunehmend auch industrielle Steuersysteme, Kameras, Sensoren und so weiter. Damit kann ich interessante Dinge anstellen …

Was für Angriffsmöglichkeiten sehen Sie?

Hackermann: Erpressungen gewinnen an Bedeutung. Wenn eine Sportwetten-Website am Tag eines Großereignisses nicht zu erreichen war, dann bekam der Betreiber Probleme – und bezahlte dann das nächste Mal lieber eine Art Schutzgeld. Oder es könnte heute ein Hochofen aus unerklärlichen Gründen runterfahren. Netzwerkkameras sind auch interessant. Aber die nutze ich nur zur Unterhaltung, denn ich arbeite allein. Um daraus Profit zu schlagen, bräuchte man ein Team.

Haben Sie Angst, erwischt zu werden?

Hackermann: Im Prinzip nicht. Die meisten sind ja froh, wenn ihre Systeme laufen, Logfiles werden da nicht geprüft. Und selbst wenn, dann steht da irgendeine IP drin von irgendeinem zufällig gewählten Proxy im Ausland, den ich gerade genutzt hatte. Die Daten anschließend zu Geld zu machen, ist jedenfalls riskanter, als an sie ranzukommen.

Was halten Sie vom neuen IT-Sicherheitsgesetz?

Hackermann: Das Gesetz ist für mich natürlich schlecht, weil es langfristig zu einer besseren Absicherung aller Unternehmen führen wird. Aber eigentlich wundere ich mich, dass es nicht viel früher gekommen ist. In der Übergangsphase wird aber sicher noch einiges möglich sein. Außerdem gibt es ja noch die Firmen, für die das Gesetz nicht gilt oder die es nicht korrekt umsetzen. Und eigentlich findet man immer einen Mitarbeiter, dem man einen Trojaner unterschieben kann, um so an die Daten auf seinem PC oder ins Firmennetz zu kommen. Was man so hört, hat das ja auch im Bundestag funktioniert. Dann klappt das auch in Unternehmen, egal wie groß.

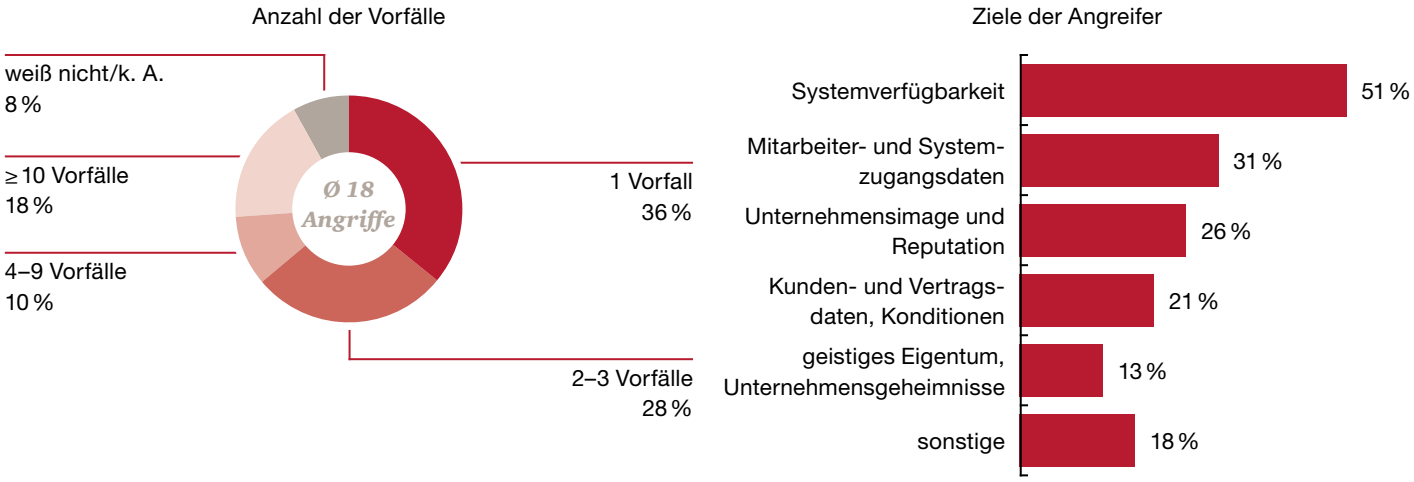
Um abzuschätzen, wie gut Mittelständler in Deutschland gegen solche Risiken gewappnet sind, haben wir in diesem Jahr erneut 400 mittelständische Unternehmen mit bis zu 1.000 Mitarbeitern von einem unabhängigen Marktforschungsinstitut zu ihrer Informationssicherheit befragen lassen. Auskunft gaben dabei vor allem leitende Angestellte, die für diesen Bereich verantwortlich zeichnen, wie Chief Information Officer (CIO), Datenschutzbeauftragte oder Compliance-Manager. Ein wichtiger Aspekt war dabei das neue IT-Sicherheitsgesetz. Es enthält regulatorische Vorgaben für Betreiber sogenannter kritischer Infrastrukturen, bei deren Störung Versorgungsengpässe oder Gefahren für die öffentliche Sicherheit drohen.

B Cyberattacken und ihre Ziele

Cyberangriffe werden immer komplexer, professioneller und zielgerichteter. Sie sind nicht erst in den vergangenen Monaten zu einer Bedrohung für mittelständische Unternehmen geworden. Um das Risiko richtig einschätzen und entsprechende Maßnahmen ergreifen zu können, ist es wichtig, die Angriffsziele der Cyberkriminellen auszumachen. Bei den befragten Mittelständlern stellt die Systemverfügbarkeit das häufigste Ziel dar (51 %), gefolgt von Mitarbeiter- und Systemzugangsdaten (31 %) sowie Unternehmensimage und Reputation (26 %). Dagegen zielen nur 13 % der Angriffe auf geistiges Eigentum und Unternehmensgeheimnisse.

Abb. 1 Anzahl der Vorfälle und Ziele der Angreifer

„Wie viele unterschiedlich Vorfälle gab es 2014?“ und „Was waren die primären Ziele der Angreifer?“



Den typischen Cyberangriff gibt es nicht, wie das breite Spektrum der Attacken beweist. Jedes Unternehmen muss also für sich herausfinden, wo bei ihm die für Angreifer wertvollsten Assets liegen, und seine Informationssicherheit darauf ausrichten. Basierend auf internationalen Vergleichswerten[2] dürften Übergriffe auf Kundendaten und Vertragskonditionen sowie geistiges Firmeneigentum in den kommenden Jahren deutlich zunehmen. Das gilt vor allem auch für den Mittelstand, denn gerade kleine und mittelgroße Firmen bemerken in vielen Fällen noch nicht einmal, wenn geistiges Eigentum entwendet wird.

[2] Vgl. PwC, The Global State of Information Security® Survey 2014 – Defending yesterday, September 2013.

C Das Ausmaß der Gefahr

Obwohl kein Unternehmen gern zugibt, zum Ziel eines Cyberangriffs geworden zu sein, sind 10 % der befragten Betriebe allein im vergangenen Jahr mindestens einmal Opfer eines Cyberangriffs geworden. Unter ihnen sind Unternehmen der Branchen Technologie, Medien und Telekommunikation (17 %) sowie Einzelhandel und Konsumgüter (12 %) besonders häufig vertreten. Hinzu kommen 5 %, die nicht wissen, ob es einen Cyberangriff auf sie gab; hier sind vor allem auch Transport- und Logistikbetriebe betroffen (15 %).

Der finanzielle Schaden, der den Unternehmen aus Cyberangriffen entstanden ist, beläuft sich laut unserer Befragung durchschnittlich auf etwa 80.000 Euro, in Einzelfällen betrug er sogar mehr als eine halbe Million Euro. Das ist ein dramatischer Anstieg: Im Vorjahr nannten 89 % der Unternehmen, die den Schaden überhaupt beziffern konnten, eine Summe von weniger als 10.000 Euro. Bei 60 % der Befragten lag überhaupt kein monetärer Schaden vor. In der aktuellen Studie liegt die Zahl der Unternehmen mit einem Schaden von weniger als 10.000 Euro nur noch bei 58 % – und damit um 31 Prozentpunkte niedriger.

Insgesamt fällt es den Unternehmen immer schwerer, den finanziellen Schaden einzuschätzen. Die Zahl der Befragten, die dazu keine genauen Angaben machen können, hat sich von 12 % im Vorjahr auf heute 33 % erhöht. Möglicherweise ist dies darauf zurückzuführen, dass die Angriffe raffinierter und komplexer geworden sind. Beeinträchtigt eine Attacke nur ein einzelnes IT-System, ist es vergleichsweise einfach, die finanziellen Folgen abzuschätzen: Wenn etwa die Produktion für mehrere Stunden ausfällt, lassen sich die Kosten für Lieferverzögerungen und Vertragsstrafen sowie der zusätzliche Arbeitsaufwand für Workarounds und die Beseitigung der Störung relativ leicht taxieren. Fallen in Unternehmen jedoch ganze Netzwerke aus, bei denen eine Vielzahl von Systemen, Abteilungen und Mitarbeitern betroffen sind, ist es aufwendig, den Schaden zu berechnen. Reputationsschäden, die entstehen, wenn vertrauliche Daten (Mitarbeiterdaten, Kundendaten, strategische Informationen) in fremde Hände gelangen, lassen sich sowieso nur schwer fundiert abschätzen. Ein Reputationsschaden bei kleinen oder spezialisierten Firmen kann ungleich schwerere Folgen haben, denn sie können daraus resultierende Umsatzeinbußen oft schlechter kompensieren als große, diversifizierte Unternehmen.

Handlungsempfehlung

Um solche Schäden zu vermeiden, kann es sich als hilfreich erweisen, wenn Unternehmen sogenannte Disaster-Recovery-Pläne vorhalten, um im Fall einer Krise die Fortführung ihres Unternehmens sicherzustellen.

Auch mittelständische Unternehmen sollten die Risiken von Cyberangriffen ernst nehmen. Doch das ist, wie unsere Studie zeigt, noch längst nicht der Fall: Nur etwa ein Fünftel der befragten Unternehmen ist gegen Cyberrisiken versichert. Fast die Hälfte (49 %) hat noch kein Managementsystem für Informationssicherheit und nur 17 % haben einen IT-Grundschutz nach ISO 27001.

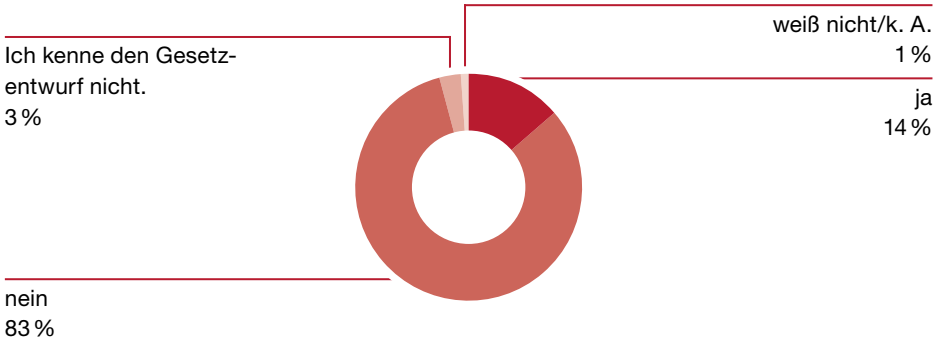
D Das IT-Sicherheitsgesetz

Verbindliche Regelungen und Gesetze für Schutzmaßnahmen zur Informationssicherheit gab es bisher nur vereinzelt (z. B. Telemediengesetz, Bundesdatenschutzgesetz) und speziell für bestimmte Branchen (z. B. Finanzdienstleistungen) oder Bereiche (z. B. Transport und Logistik). Mit dem Ende Juli 2015 in Kraft getretenen IT-Sicherheitsgesetz (IT-SiG) gibt es in Deutschland erstmals ein Bündel regulatorischer Vorgaben zur Informationssicherheit, die bis zum 13. Juni 2017 umgesetzt werden müssen. Das Gesetz gilt für Betreiber sogenannter kritischer Infrastrukturen. Darunter fallen alle Unternehmen und Organisationen, 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". Das IT-SiG teilt die betroffenen Branchen dazu in die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen auf. Die Bundesregierung geht derzeit davon aus, dass etwa 2.000 Unternehmen in Deutschland von diesem Gesetz betroffen sind. Andere Schätzungen gehen dagegen von bis zu 5.000 Unternehmen aus.[3]

Laut IT-SiG müssen diese Unternehmen
- einen Informationssicherheitsbeauftragten benennen, der jederzeit für das Bundesamt für Sicherheit in der Informationstechnik als Ansprechpartner zur Verfügung steht (inkl. Stellvertreterregelung);
- ein Informationssicherheitsmanagementsystem (ISMS) zur Identifikation von Cyberangriffen etablieren, das sich an einem gängigen Standard orientiert;
- eine Meldestelle einrichten, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) über Cyberangriffe informiert.

Das IT-SiG bezieht sich auch auf mittelständische Unternehmen. In unserer Studie gehen 14 % der Befragten davon aus, von den neuen Regelungen betroffen zu sein. Bei größeren mittelständischen Unternehmen mit 500 bis 1.000 Mitarbeitern liegt dieser Anteil mit 19 % deutlich höher. Zwar stand der genaue Gesetzestext zum Zeitpunkt unserer Befragung noch nicht fest, doch die wesentlichen Inhalte waren den Teilnehmern bekannt.

Abb. 2 Ist Ihr Unternehmen vom IT-Sicherheitsgesetz (IT-SiG) betroffen?



[3] Vgl. www.heute.de/umstrittenes-it-sicherheitsgesetz-thema-auf-bsi-konkress-38500542.html.

Bei der Frage, inwieweit betroffene Unternehmen bereits die drei zentralen Vorgaben – Sicherheitsbeauftragter, Meldestelle und ISMS – erfüllen, ergibt sich ein heterogenes Bild: So verfügen 24 % bereits über einen Informationssicherheitsbeauftragten als Ansprechpartner für das BSI. Vor allem die Branchen Finanzdienstleistungen und Versicherungen sind hier führend. Nachholbedarf herrscht dagegen im Bereich Transport und Logistik.

Im Hinblick auf eine Meldestelle für Cyberangriffe ist es für 38 % der betroffenen Unternehmen kein Problem, eine solche Stelle einzurichten, für nur 7 % ist dies derzeit noch nicht möglich. Unternehmen aus den Branchen Gesundheitswesen und Pharma, Finanzdienstleistungen und Versicherungen und Energie sind bereits gut vorbereitet, Nachholbedarf besteht auch hier in Unternehmen der Transport- und Logistikbranche sowie Technologie, Medien und Telekommunikation.

Den größten Investitionsbedarf erfordern Einführung und Betrieb eines funktionierenden ISMS, das einem der gängigen Standards entspricht. Das IT-SiG schreibt für jedes betroffene Unternehmen ein solches System vor, damit Cyberangriffe erkannt, Maßnahmen zu deren Abwehr eingeleitet und Schwachstellen identifiziert und behoben werden. Doch gerade mittelständische Unternehmen gehen dieses Thema eher verhalten an, weil entsprechende Projekte personelle und finanzielle Ressourcen binden und keinen unmittelbaren Nutzen für den normalen Geschäftsbetrieb bieten.

Auf Dauer können Unternehmen ihre IT-Sicherheit jedoch nur mit einem ISMS gewährleisten. 41 % der befragten Unternehmen haben bereits ein zertifiziertes ISMS. Im Finanzdienstleistungs- und Versicherungssektor, für den schon länger eine Verpflichtung durch die Bundesanstalt für Finanzdienstleistungsaufsicht besteht, sind es – wenig überraschend – schon 85 %. Trotzdem nennen 54 % der Befragten, die bereits ein ISMS eingerichtet haben, für die Implementierung und Zertifizierung eher interne Gründe. Nur bei 35 % spielen regulatorische Vorgaben die entscheidende Rolle zur Einführung eines ISMS. Bei den Investitionen in IT-Sicherheit hingegen zeichnet sich ein anderes Bild ab, wo knapp 80 % der befragten Unternehmen regulatorische Anforderungen als Grund von Investitionen angeben. Das lässt den Rückschluss zu, dass Informationssicherheit nach wie vor eher als IT-Aufgabe aufgefasst wird.

Unsere Umfrage zeigt, wie groß bei Mittelständlern die Unterschiede im Hinblick auf das Thema Cybersicherheit sind. Obwohl nur 14 % der befragten Unternehmen angeben, vom IT-SiG betroffen zu sein, gibt es durchaus Branchen, in denen signifikant mehr Unternehmen Cybersicherheits-Maßnahmen schon länger diskutieren und umsetzen als in anderen Branchen. Zugleich haben mehr als die Hälfte der befragten Unternehmen (55 %), die von dem Gesetz betroffen sind, bisher noch keine Schritte eingeleitet, um die Vorgaben zu erfüllen.

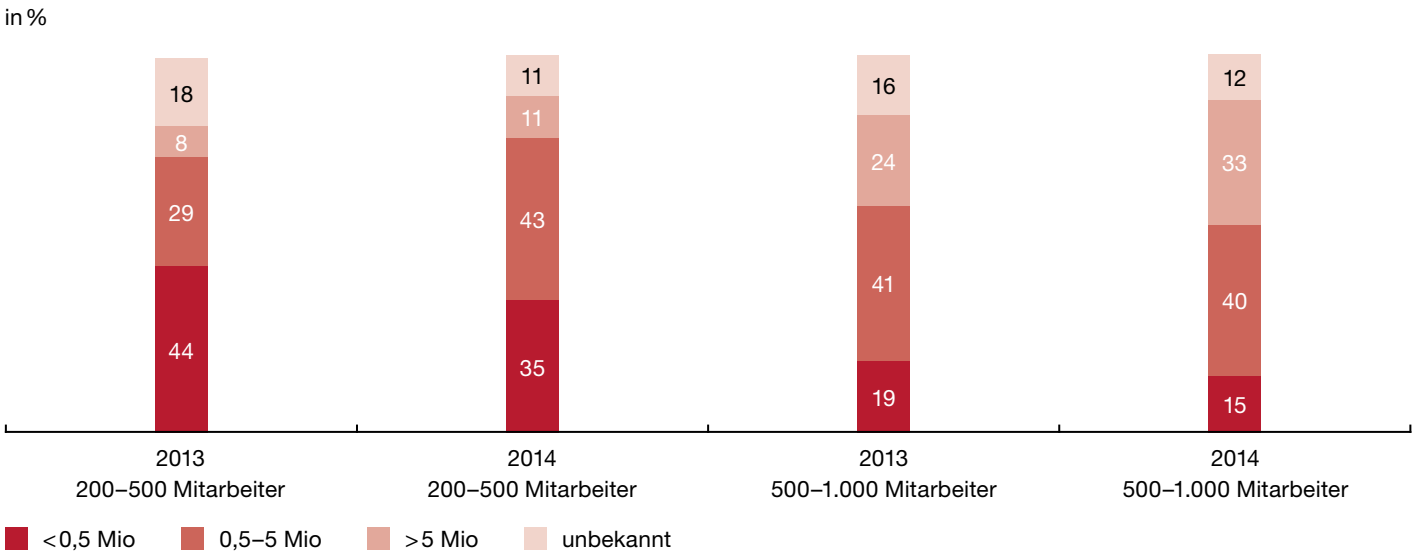
Handlungsempfehlung

Die Unternehmen sollten sich dem Gesetz nicht versperren, sondern es als Chance begreifen, um sich gegen Cyberattacken zu schützen. Auch sind sich viele Unternehmen noch nicht bewusst, dass sie vom IT-SiG betroffen sind, so dass bei ihnen Handlungsbedarf besteht.

E Die Höhe der IT-Budgets

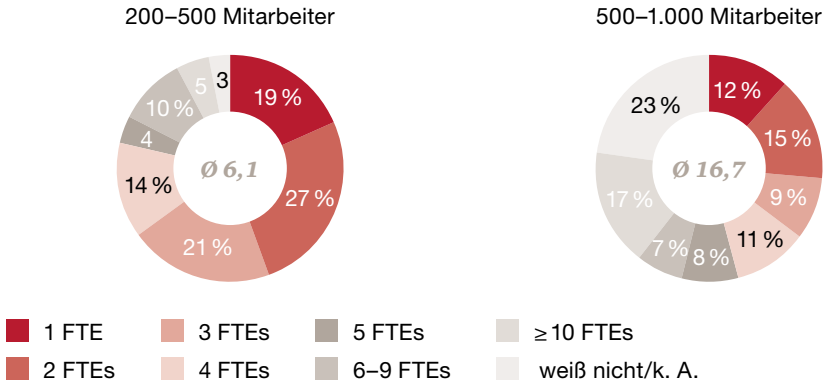
Unternehmen räumen der Informationssicherheit einen immer höheren Stellenwert ein. Das zeigt sich bereits an der Höhe des IT-Budgets. So ist die Anzahl der mittelständischen Unternehmen mit einem Budget von einer halben bis zu 5 Millionen Euro gegenüber unserer letzten Befragung um 10 % gestiegen.

Abb. 3 Höhe des IT-Budgets



Die Zahl der Mitarbeiter, die im Bereich Informationssicherheit beschäftigt sind, beläuft sich im Schnitt auf knapp 11 Full Time Equivalents (FTEs). Bei großen mittelständischen Unternehmen mit 500 bis 1.000 Mitarbeitern sind es fast 17 FTEs; mittelständische Unternehmen mit 200 bis 500 Mitarbeitern beschäftigen im Schnitt 6 FTEs im Bereich Informationssicherheit. Dies ist eine solide Basis, aber noch ausbaufähig.

Abb. 4 Personalausstattung im Bereich Informationssicherheit



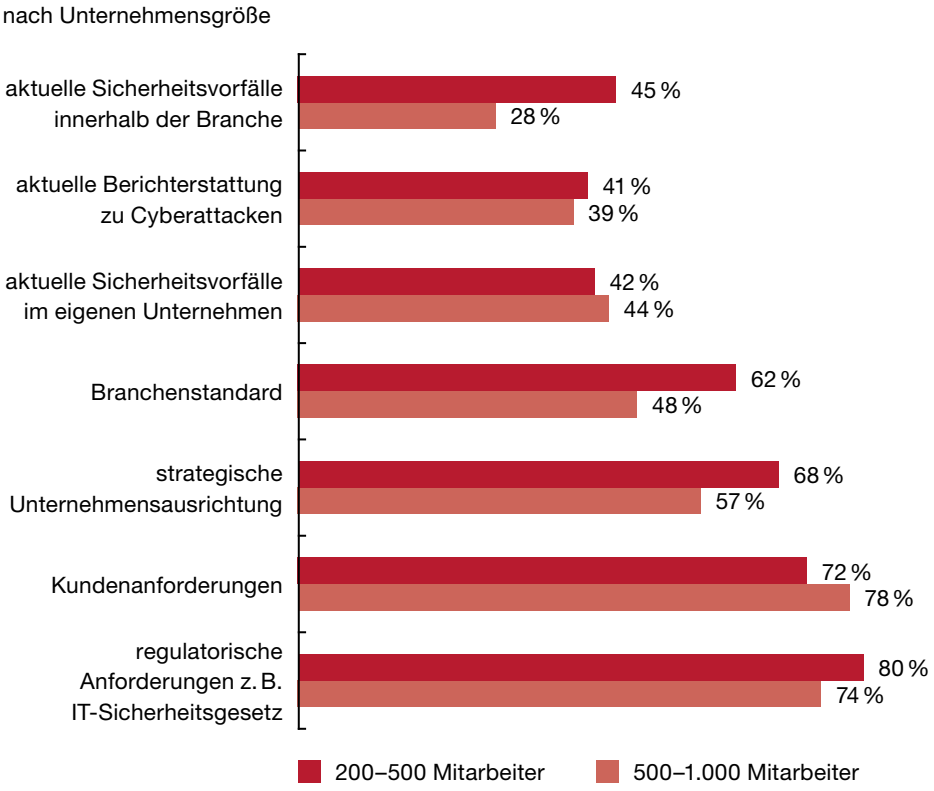
Die Höhe des jährlichen IT-Budgets hängt erwartungsgemäß entscheidend von der Unternehmensgröße ab und beträgt bei drei Viertel der befragten Mittelständler weniger als 5 Millionen Euro. Bei einem Drittel umfasst das IT-Budget maximal eine halbe Million Euro. Dagegen gibt es einige spezialisierte Unternehmen, die große Summen investieren: 7 % der Mittelständler halten ein Budget von mindestens 50 Millionen Euro vor, darunter sind sogar einige mit einem Budget von mindestens 500 Millionen Euro (2 %). Dabei handelt es sich ausnahmslos um große mittelständische Unternehmen mit 500 bis 1.000 Mitarbeitern und Umsätzen von mehr als 500 Millionen Euro. Im Branchenvergleich liegen die Budgets im Bereich Einzelhandel und Konsumgüter im Schnitt über jenen von Industrie- oder Dienstleistungsunternehmen.

Ausgelöst werden diese Investitionen in die IT-Sicherheit überwiegend durch gesetzliche Vorgaben oder Anforderungen von Kunden. 74 % der Unternehmen mit 200 bis 500 Mitarbeitern und 80 % der Gesellschaften mit 500 bis 1.000 Mitarbeitern nennen regulatorische Anforderungen wie das IT-SiG als entscheidenden Grund. 2014 waren es dagegen nur 45 % (200 bis 500 Mitarbeiter) bzw. 52 % (500 bis 1.000 Mitarbeiter). Vor allem bei Unternehmen aus den als kritisch geltenden Bereichen Energie sowie Finanzdienstleistungen und Versicherungen macht sich der regulatorische Druck bemerkbar. Sie alle führen in diesem Zusammenhang das IT-Sicherheitsgesetz oder das Kreditwesengesetz (KWG) an. Auffällig ist, dass der Branchenstandard sowie aktuelle Sicherheitsvorfälle innerhalb der Branche bei den größeren Mittelständlern einen deutlich höheren Stellenwert einnehmen als bei den kleineren. Dies lässt den Rückschluss zu, dass die größeren Unternehmen (> 500 Mitarbeiter) stärker mit den Branchenverbänden interagieren, um sich bzgl. Cyberrisken und -lösungen zu informieren.

Handlungsempfehlung

Auch kleinere Firmen sollten diese Informationsquellen stärker nutzen, um sich insbesondere über branchenspezifische Bedrohungen aber auch über Lösungen auszutauschen, die für den Mittelstand realisierbar sind.

Abb. 5 Gründe, in Informationssicherheit zu investieren



Handlungsempfehlung

Um gegen Cyberattacken gewappnet zu sein, sollten Unternehmen nicht nur einen definierten Anteil ihres Budgets für Sicherheitsmaßnahmen vorhalten, sondern die Sicherheit bei allen Maßnahmen berücksichtigen. Zudem können sie derzeit einen Imagevorteil erzielen, indem sie die Investitionen in die IT-Sicherheit bei der Zertifizierung nach außen kommunizieren.

F Cybersicherheit ist Chefsache

IT-Sicherheit kann in Unternehmen nur dann erreicht werden, wenn das Thema von der Geschäftsführung ins Unternehmen getragen wird und eine regelmäßige Berichterstattung gewährleistet ist. In 92 % der befragten mittelständischen Unternehmen mit 200 bis 500 Mitarbeitern wird die Unternehmensleitung direkt informiert, bei Betrieben mit mehr als 500 Mitarbeitern sind es 88 %. Das Thema Cybersicherheit wird offensichtlich mehr und mehr zur Chefsache: 43 % der Unternehmen mit 200 bis 500 Mitarbeitern, in denen im vergangenen Jahr noch nicht automatisch informiert wurde, haben dies inzwischen geändert; bei den großen Unternehmen mit 500 bis 1.000 Mitarbeitern liegt der Anteil bei 48 %.

Insgesamt berichten die in der Studie befragten Verantwortlichen für Informationssicherheit in neun von zehn Fällen direkt an die Unternehmensleitung. Jeder zweite IT-Entscheider stimmt sich zudem mit dem Datenschutzbeauftragten ab. Vor allem in größeren Unternehmen gibt es noch weitreichendere Berichtspflichten. In den Branchen Energie und Automobil geht der Bericht immer direkt an die Geschäftsführung.

Handlungsempfehlung

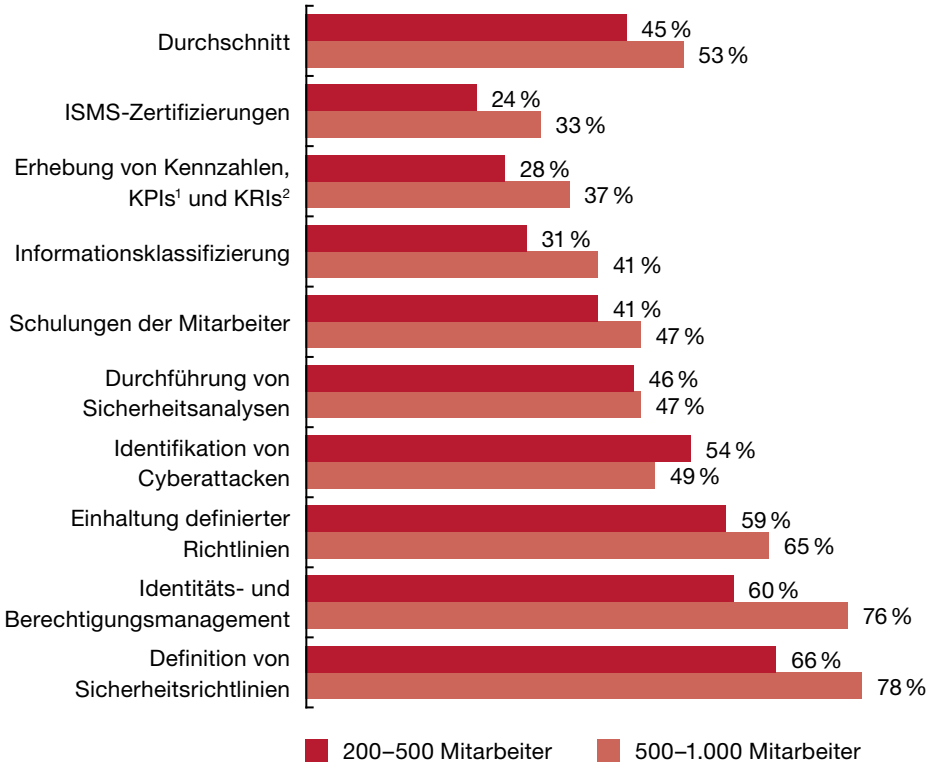
Im Bereich Gesundheitswesen und Pharma ist mit 82 % Umsetzung und im Bereich Technologie, Medien und Telekommunikation mit 80 % Umsetzung noch Verbesserungspotenzial vorhanden. Das heißt, auch diese Unternehmen sollten IT-Sicherheit zur Chefsache machen und mit der notwendigen Ernsthaftigkeit betreiben – nicht zuletzt auch vor dem Hintergrund des IT-SiG.

Abb. 6 Bericht direkt an die Geschäftsführung

G Ansatzpunkte für Verbesserungen

Nach Einschätzung der Verantwortlichen gehören die Erhebung von Kennzahlen sowie Mitarbeiterschulungen und Informationsklassifizierung zu den vernachlässigten Aspekten im Rahmen des Informationssicherheitsprozesses. Die Ergebnisse im Einzelnen: 72 % der Beauftragten schätzen die Sicherheitsrichtlinien in ihrem Unternehmen als gut oder sehr gut ein, aber nur 32 % würden dies für die Kennzahlen sagen. Das Identitäts- und Berechtigungsmanagement (68 %), die Einhaltung definierter Richtlinien (62 %) und die Identifikation von Cyberattacken (51 %) werden überwiegend als gut oder sehr gut bewertet. Den eigenen Mitarbeiterschulungen stellen nur 44 % der befragten Unternehmen die Note „gut" aus, bei der Informationsklassifizierung sind es nur 36 %.

Abb. 7 Gute oder sehr gute Umsetzung innerhalb des Informationssicherheitsprozesses

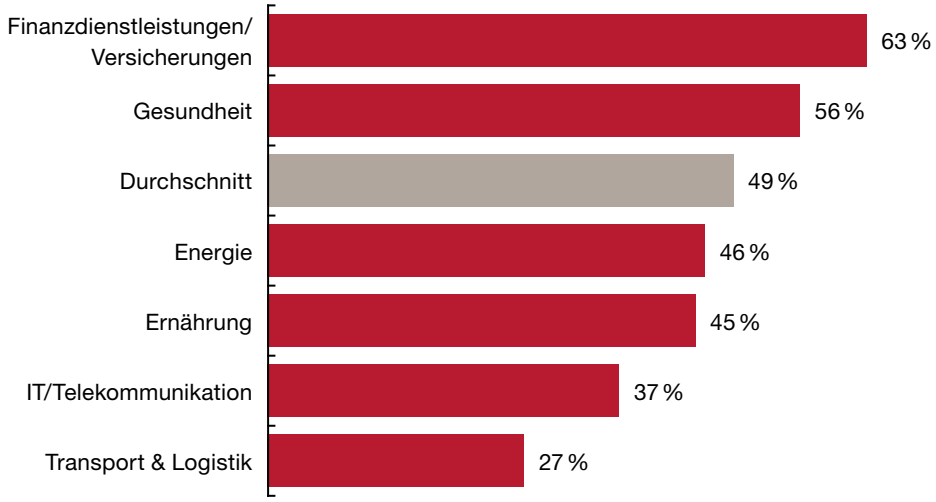


[1] Key Performance Indicator
[2] Key Risk Indicator

Die Zahlen zeigen, dass vor allem kleinere Unternehmen Nachholbedarf haben.

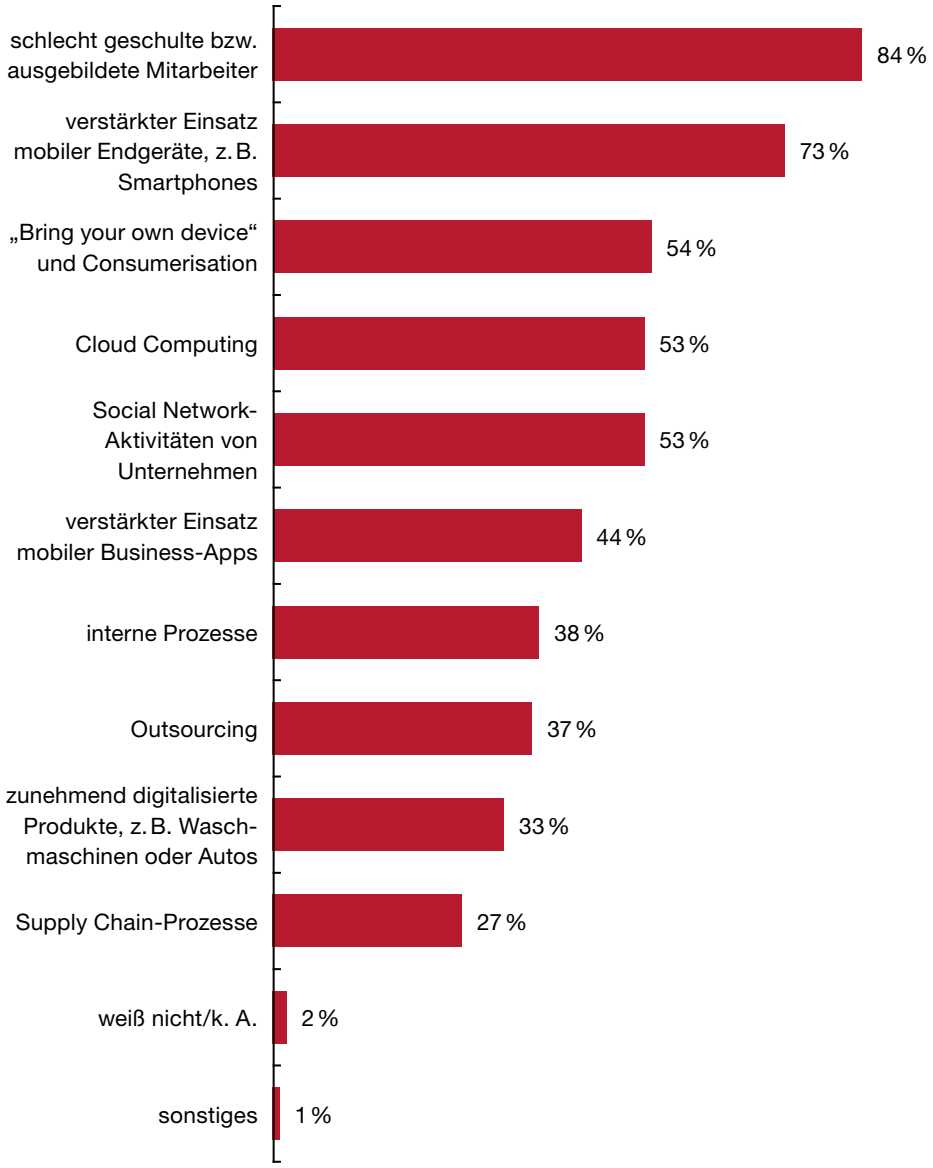
Abb. 8 Unternehmen mit „guter“ oder „sehr guter“ Umsetzung des Informationssicherheitsprozesses

nach Sektoren



Der Finanzdienstleistungs- und Versicherungssektor ist mit 63 % bei der Umsetzung schon weiter; Betriebe aus dem Transport- und Logistiksektor bilden mit 27 % das Schlusslicht. Trotz allem ist die Quote mit einer zumindest „guten“ Umsetzung des Informationssicherheitsprozesses insgesamt zu niedrig.

Abb. 9 Worin Firmen Sicherheitsrisiken sehen



Schlecht ausgebildete und unzureichend geschulte Mitarbeiter werten die befragten Unternehmen als größtes Sicherheitsrisiko, dicht gefolgt vom verstärkten Einsatz mobiler Endgeräte wie Smartphones. Weitere heikle Aspekte sind private Laptops in Unternehmensnetzwerken („Bring your own device“), Social-Network-Aktivitäten und Cloud Computing. Zwar wird der Einsatz von Social Media gerade im Marketing immer wichtiger, doch zugleich befürchten Unternehmen aufgrund fehlender Erfahrung mit diesen relativ neuen Technologien große Risiken.

In allen Bereichen der Informationssicherheit ist Schulungsbedarf vorhanden, insbesondere in Unternehmen mit 200 bis 500 Mitarbeitern. Hier kann mit vergleichsweise geringen Investitionen sehr viel bewirkt werden, denn oft bilden Unachtsamkeiten einzelner Mitarbeiter das Einfalltor für Cyberattacken.

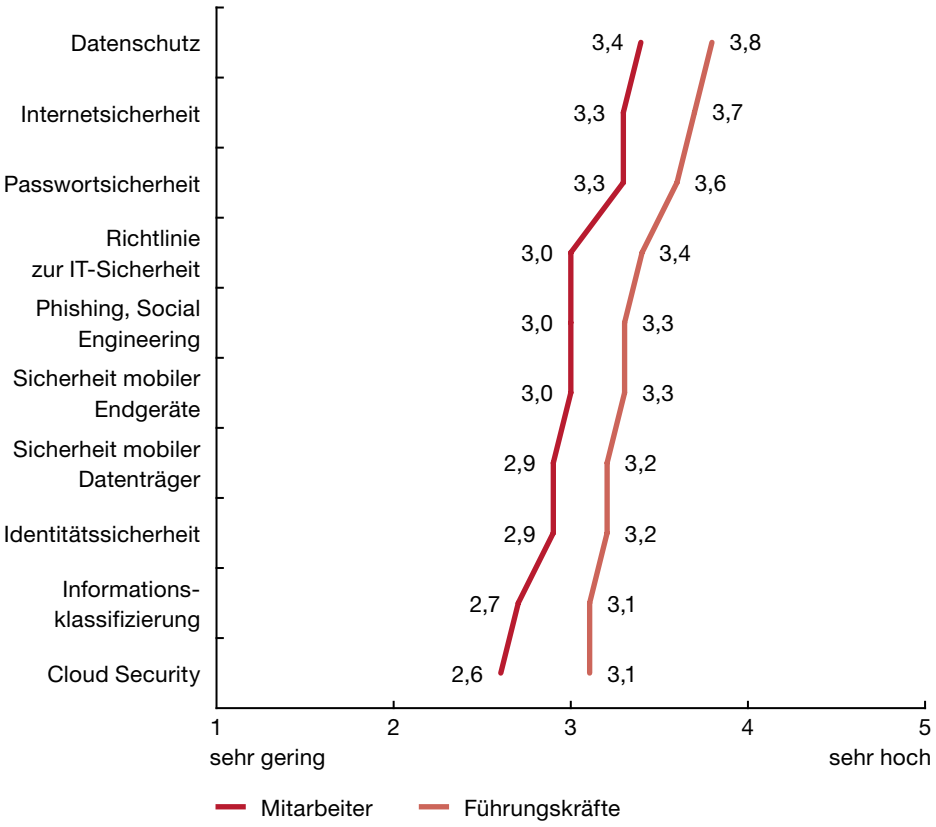
Die bestehenden internen Schulungen, die Mitarbeiter auf IT-Sicherheitsrisiken hinweisen sollen, beurteilen nur 6 % der Unternehmen als „sehr gut“, während 17 % sie mit „schlecht“ oder „sehr schlecht“ bewerten. Größere Unternehmen sind in diesem Punkt tendenziell besser aufgestellt: 87 % der befragten großen mittelständischen Unternehmen mit 500 bis 1.000 Mitarbeitern bewerten ihre Mitarbeiterschulungen als „mittel“ oder „besser“; bei Unternehmen mit 200 bis 500 Mitarbeitern sind es nur 77 %.

Auch in der Sensibilisierung von Mitarbeitern zu IT-Sicherheitsthemen sehen die befragten Verantwortlichen Potenzial für Verbesserungen: Weder bei Führungskräften noch bei Mitarbeitern wird ein Sensibilisierungsgrad genannt, der über den Wert von 3,8 hinausgeht – gemessen an einer Skala von 1 für „sehr gering“ bis 5 für „sehr hoch“. Zwar schneiden die Führungskräfte aus Sicht der befragten IT-Vertreter besser ab als die übrigen Mitarbeiter, aber das nur auf niedrigem Niveau: So werden nur 46 % der Führungskräfte und 32 % der Mitarbeiter als „hoch“ oder „sehr hoch“ sensibilisiert eingestuft.

Abb. 10 Sensibilisierung für Themen der Informationssicherheit

„Wie schätzen Sie die Sensibilisierung der Führungskräfte … ein?“ und „Wie schätzen Sie die Sensibilisierung der Mitarbeiter … ein?“

Durchschnittswerte

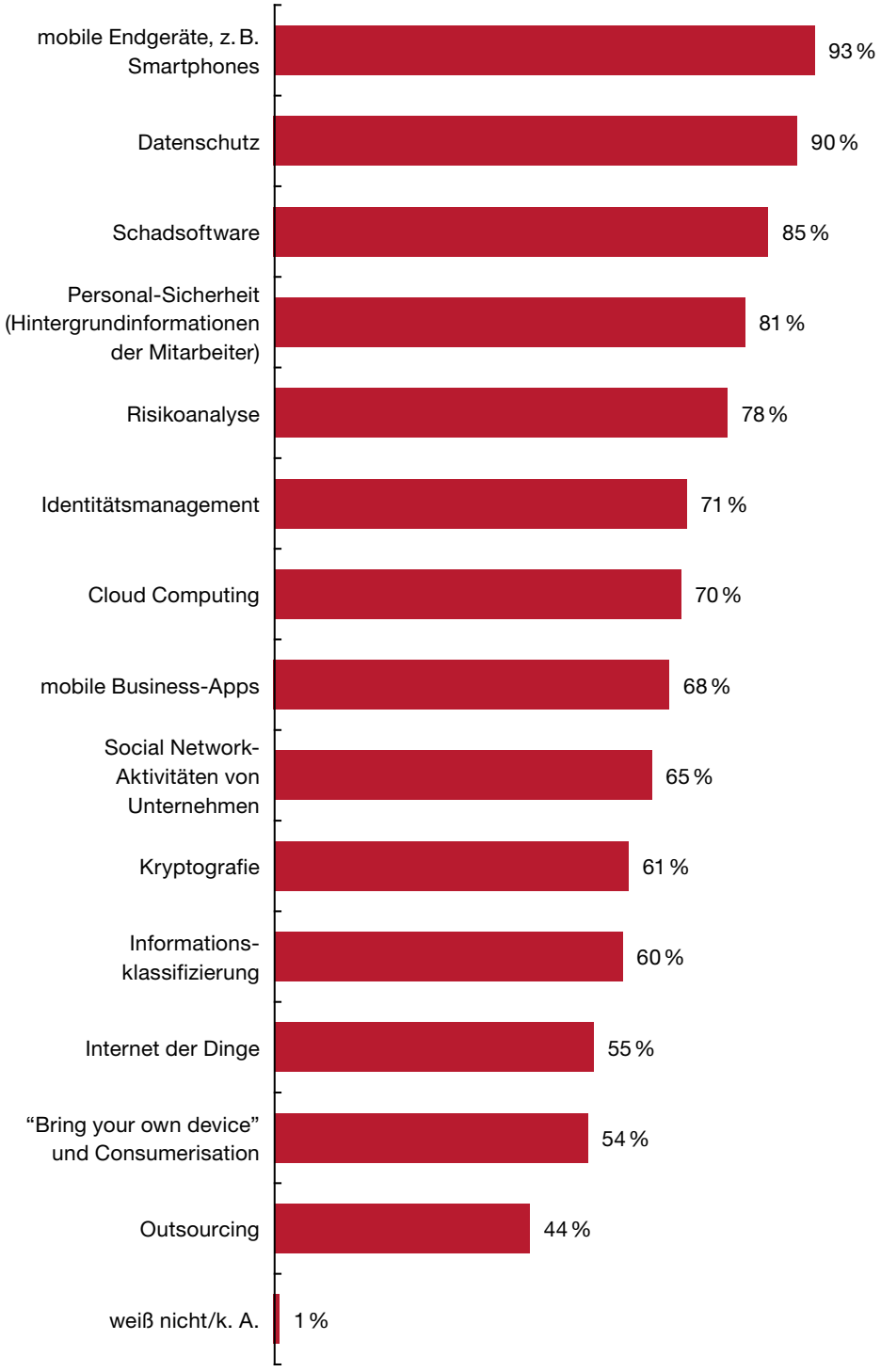


Bei Fragen des Datenschutzes sowie Internet- und Passwortsicherheit sind Unternehmen offensichtlich schon hellhöriger: 58 % der Führungskräfte und fast die Hälfte der Mitarbeiter werden jeweils als mindestens „gut sensibilisiert“ eingestuft. Die Sicherheitsklassifizierung von Inhalten oder Cloud Security sind dagegen häufig noch kein Thema in den Unternehmen. Hier gaben nur 29 % bzw. 19 % der Befragten einen hohen oder sehr hohen Sensibilisierungsgrad an.

In einigen Punkten können sich Dienstleistungsunternehmen positiv absetzen – vor allem bei Datenschutz, Passwortsicherheit, Phishing bzw. Social Engineering sowie bei der Sicherheit von mobilen Endgeräten und Speichermedien.

Mobile Endgeräte sind unter dem Aspekt der Informationssicherheit stärker in den Fokus der Aufmerksamkeit gerückt. Während im Vorjahr nur 24 % der Entscheider dieses Thema als wichtig erachtet haben, sind es in der aktuellen Studie 93 %. Das Thema Cloud Computing, das im vergangenen Jahr die Liste der zukünftig relevanten IT-Themen anführte, ist inzwischen im Mittelfeld wiederzufinden.

Abb. 11 Zukünftig relevante IT-Themen



Überraschend ist, dass das Thema „Bring your own device“ an vorletzter Stelle rangiert, obwohl es insgesamt als dritt größtes Risiko eingestuft worden ist (vgl. Abbildung 9). Selbst in Betrieben, die als kritische Infrastruktur gelten, werden die Themen Outsourcing und Kryptografie noch häufiger genannt als Identitäts-management, Internet der Dinge und „Bring your own device“ – trotz der Risiken, die der Einsatz privater Geräte am Arbeitsplatz birgt. Gerade bei der Nutzung privater Geräte ist eine weitere Sensibilisierung notwendig, um auf die Gefahren hinzuweisen und entsprechende Maßnahmen einzuleiten.

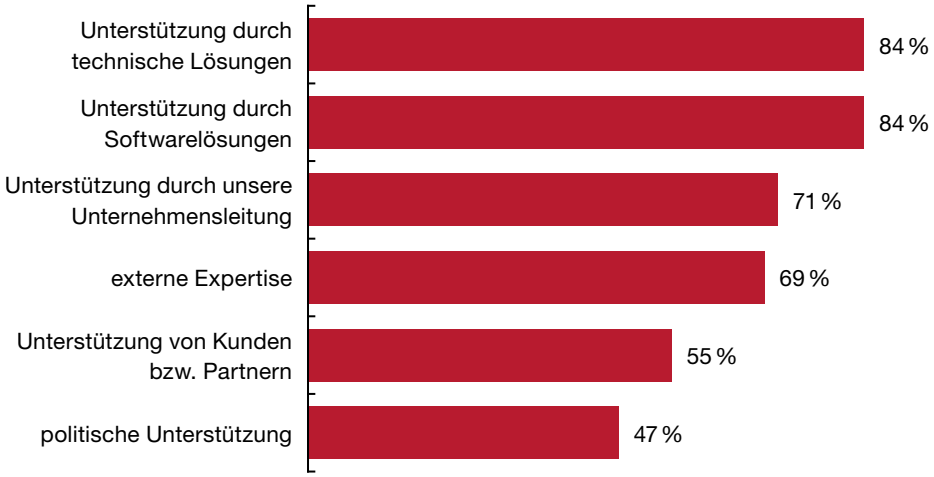
H Zusammenfassung und Fazit

Mittelständischen Betrieben wird zunehmend bewusst, dass Cyberkriminalität ein reales Risiko darstellt. Die hierdurch verursachten Schäden haben sich im vergangenen Jahr deutlich erhöht. Viele Unternehmen stocken daher ihr Budget für Sicherheitstechnik auf und das Thema wird zunehmend zur Chefsache. Der Hauptgrund für Sicherheitsmaßnahmen ist aber nicht die Angst vor Schäden; vielmehr sind Kundenwünsche und regulatorische Anforderungen hier das wesentliche Motiv. So kann eine Zertifizierung im Bereich der IT-Sicherheit derzeit noch einen Imagevorteil generieren. Die Etablierung eines ISMS wendet dabei nicht nur mögliche Schäden ab; das System kann dem Unternehmen darüber hinaus auch helfen, sich einen Wettbewerbsvorteil zu verschaffen und die eigenen Geschäftsprozesse hinsichtlich Vertraulichkeit, Integrität und Zuverlässigkeit nachhaltig zu verbessern. Zertifizierungen werden künftig jedoch mehr und mehr vorausgesetzt werden; ihr Fehlen wird so zunehmend zum Hindernis und damit letztlich auch zum Wettbewerbsnachteil.

Insgesamt verfügt nur ein relativ kleiner Anteil der mittelständischen Unternehmen schon heute über einen guten Informationssicherheitsprozess. Während Branchen wie Finanzdienstleistungen und Versicherungen – getrieben von regulatorischen Vorgaben – die Implementierung der nötigen Prozesse schon weitgehend umgesetzt haben, gibt es bei Unternehmen aus den Bereichen Transport und Logistik sowie Technologie, Medien und Telekommunikation einen deutlichen Nachholbedarf, der insbesondere vor dem Hintergrund des Inkrafttreten des IT-Sicherheitsgesetzes umso dringlicher erscheint.

Abb. 12 Unterstützungsbedarf in Bezug auf das IT-Sicherheitsgesetz

An welchen Stellen sehen Sie Unterstützungsbedarf bei der Erfüllung der Anforderungen aus dem IT-Sicherheitsgesetz?



Cybersicherheit wird von den Unternehmen bisher vorrangig als ein rein technisches Problem begriffen. Sie wünschen sich Unterstützung, um die richtigen Hard- und Softwarelösungen für sich zu finden, auch durch externe Berater. Dagegen werden die Sensibilisierung und Schulung der Mitarbeiter im Hinblick auf Cybersicherheit viel zu sehr vernachlässigt. Schlecht geschulte Mitarbeiter werden

als häufigstes Sicherheitsrisiko betrachtet, aber in allen Bereichen der Informationssicherheit ist Schulungsbedarf vorhanden – nur 6 % der Unternehmen bewerten ihre Schulungen als sehr gut, während 17 % sie als schlecht oder sehr schlecht bewerten. Es werden nur 46 % der Führungskräfte und 32 % der Mitarbeiter als hoch oder sehr hoch sensibilisiert eingestuft. Gerade in diesem Bereich ließe sich mit verhältnismäßig geringem Aufwand viel erreichen.

Das Thema „Bring your own device" ist ein IT-Risiko, das von mittelständischen Firmen derzeit noch völlig unterschätzt wird – vielleicht auch deswegen, weil es bei vielen noch nicht zum Arbeitsalltag gehört. Sich von privaten Endgeräten in Firmennetze einzuloggen, wird im Zuge neuer Arbeitszeitmodelle und Home-Office-Lösungen in Zukunft immer häufiger der Fall sein. Ein ideales Einfallstor für Hacker, wenn die Firmen sich nicht vorsehen.

Die Bundesregierung hat mit dem Ende Juli 2015 in Kraft getretenen IT-SiG eine wichtige und öffentlichkeitswirksame Weiche in puncto Wahrnehmung und Umsetzung der Informationssicherheit in deutschen Unternehmen gestellt. Unter rein formalen Aspekten sind sich sowohl die Gremien und Verbände als auch die Sicherheitsspezialisten einig, dass ein solches Gesetz nicht zwingend notwendig gewesen wäre, liefern doch die bestehenden Gesetze, Verordnungen und Vorgaben ausreichend Substanz, um Unternehmen zur Umsetzung von Maßnahmen zur Informationssicherheit anzuhalten. Aufgrund wirtschaftlicher Interessen der Unternehmen wurden diese jedoch bisher häufig nicht systematisch umgesetzt.

Für Unternehmen, die kritische Infrastrukturen betreiben, ist damit nun Schluss. Diese müssen bis Mitte 2017 einen zertifizierten Sicherheitsprozess einführen – und daran wird auch die noch teilweise bestehende Unsicherheit zur konkreten Umsetzung einzelner Vorgaben des IT-Sicherheitsgesetzes nichts ändern; sie wird dies lediglich um wenige Monate verschieben. Hiervon sind auch eine Reihe namhafter mittelständischer Unternehmen, zum Beispiel in der Logistikbranche, unmittelbar betroffen. Unternehmen, deren Geschäftsmodelle sich zukünftig aufgrund der Digitalisierung disruptiv verändern werden, sind gut beraten, frühzeitig zu prüfen, ob sie durch diese Veränderungen zu einem Teil der kritischen Infrastruktur in Deutschland werden. Beispielsweise wird sich im Gesundheitssektor aufgrund des Kostendrucks das Dienstleistungsbild der Krankenhäuser massiv verändern. Heilbehandlungen werden in den häuslichen Bereich verlagert werden und die Hersteller medizinischer Überwachungs- und Versorgungsgeräte werden diese von der Anlieferung an häusliche Pflegeplätze über den Betrieb, die Entstörung und Wartung bis hin zur Wiederabholung betreuen müssen. Damit verlagert sich die kritische Infrastruktur vom Krankenhaus in den häuslichen Bereich und weitergehend in die Verantwortung von Dienstleistern – doch darauf sind diese noch nicht angemessen vorbereitet. Das IT-Sicherheitsgesetz wird also aufgrund der weiter zunehmenden Digitalisierung seinen Geltungsbereich kontinuierlich ausdehnen – in einer komplett vernetzten Welt kann nicht mehr von einer Differenzierung zwischen kritischen und nicht kritischen Infrastrukturen ausgegangen werden: Die Erwartung der Menschen an das Internet lautet schon heute: 100 % Verfügbarkeit – und das Internet der Dinge wird diese Erwartung nicht verringern.

Auch der Mittelstand wird sich kurz- bis mittelfristig mit dieser Entwicklung auseinandersetzen müssen. Operativ wird dies dazu führen, dass mittelständische Unternehmen gezwungen sein werden, die Anforderungen des IT-Sicherheitsgesetzes auch dann umzusetzen, wenn sie nicht direkt zu den kritischen Infrastrukturen gehören. Der Mittelstand wird dem Trend folgen müssen, den gehobenen Anforderungen seiner Geschäftspartner und Kunden im Bereich der Informationssicherheit gerecht zu werden – einhergehend mit dem Gewinn effektiverer und störungsresistenterer Geschäftsprozesse.

I Methodik

Diese Studie beschreibt die Ergebnisse einer Befragung von 400 Unternehmen aus Deutschland, die von einem unabhängigen Marktforschungsinstitut im Auftrag von PwC in Form von computergestützten Telefoninterviews (CATIs) auf Basis eines vollstrukturierten Fragebogens im Zeitraum vom 12. Mai bis zum 19. Juni 2015 durchgeführt wurde. Abweichend von gängigen Definitionen des Mittelstands, die Unternehmen bis zu einer Größe von 250 Mitarbeitern umfassen, wurden in dieser Studie mittelständisch geprägte Unternehmen in Deutschland mit einer Mitarbeiteranzahl von bis zu 1.000 Mitarbeitern befragt.

Das Vorgehen wurde gewählt, da selbst größere und eigentümergeführte Unternehmen häufig mittelständisch geprägt sind und die informationssicherheitsrelevanten Strukturen vergleichbar sind. Um ggf. vorhandene Unterschiede zwischen mittelständischen Unternehmen herausstellen zu können, wurde die Befragung in zwei Gruppen unterteilt. Jeweils 200 Interviews wurden mit Unternehmen mit 200 bis 500 Mitarbeiter und Unternehmen mit 500 bis 1.000 Mitarbeiter geführt.

Der Fragebogen war auf Unternehmensmitarbeiter mit IT-Verantwortung ausgerichtet, sodass die IT-Leiter den größten Teil der befragten Personen stellten. Insgesamt 84 % der Befragten waren nach eigener Aussage als IT-Direktor, Informationssicherheitskoordinator, Datenschutzbeauftragter, Chief Information Officer (CIO), Informationssicherheitsmanager, Chief Security Officer (CSO), Compliance-Manager oder Informationssicherheitsdirektor tätig.

Die Vergleiche mit dem Vorjahr beziehen sich auf die erste Ausgabe der Studie, die im März 2014 erschienen ist. Damals wurden nach derselben Methodik 406 Unternehmen befragt.

Ihre Ansprechpartner

Dr. Peter Bartels
Vorstand und Leiter des Bereichs
Familienunternehmen und Mittelstand
Tel.: +49 211 981-2176
peter.bartels@de.pwc.com

Derk Fischer
Partner für Cyber Security
Risk Assurance Solutions
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. 9.800 engagierte Menschen an 29 Standorten. 1,65 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland. Partner für Familienunternehmen und Mittelstand.