Abschlussbericht

„IT-DIENSTLEISTER ALS AKTEURE ZUR STÄRKUNG DER IT-SICHERHEIT BEI KMU IN DEUTSCHLAND“

STUDIE IM AUFTRAG DES BUNDESMINISTERIUMS FÜR WIRTSCHAFT UND ENERGIE

AUTORINNEN DER STUDIE:

CHRISTIAN KÖHLER, CHARMAINE RICKERSON, PHILIP STEINKRÜGER, ORTWIN WOHLRAB, STEFFEN KOLB, ESTHER KERN, TIM STUCHTEY, ALEXANDER SZANTO

erstellt durch
NKMG mbH & BIGS gGmbH
19.02.2021

Inhalt

1. Executive Summary

Kleine und mittlere Unternehmen (KMU) spielen eine zentrale Rolle für die Wirtschaftskraft Deutschlands. Sie stehen u.a. durch die Digitalisierung und Vernetzung ihrer Wertschöpfungsketten unter einem transformativen Druck. Die Digitalisierung von Management- und Produktionsprozessen hat auch Auswirkungen auf die Unternehmens- und IT-Sicherheit von KMU. Aufgrund ihrer kleinen oder mittleren Größe verfügen KMU selten über eigene IT-Abteilungen. Daher fehlt es ihnen vielfach an eigenen Ressourcen und Kompetenzen im Bereich der Informations- und Kommunikationstechnik, der IT-Sicherheit sowie der Informationssicherheit. Bei diesen Themen sind viele KMU somit regelmäßig auf die Hilfe externer IT-Dienstleister angewiesen. Diese IT-Dienstleister sind häufig die ersten Ansprechpartner, wenn KMU sich zusätzlich zu den IT-Services mit Fragen der IT-Sicherheit auseinandersetzen müssen.

Aus diesem Grund hat das Bundesministerium für Wirtschaft und Energie (BMWi) mit dieser Studie folgende Fragestellungen genauer untersuchen lassen:

- Wie ist die Gruppe der IT-Dienstleister zu definieren?
- Welche IT-Dienstleistungen werden den KMU angeboten (Betrachtung der Angebotsseite)?
- Wie arbeiten IT-Dienstleister und ihre (KMU-) Kunden bezüglich der IT-Sicherheit als Teil des Leistungsportfolios von IT-Dienstleistungen zusammen?
- Wie finden KMU geeignete IT-Dienstleister und nach welchen Kriterien wählen sie diese aus (Betrachtung der Nachfrageseite)?

Unternehmen mit Dienstleistungen im Bereich der Informationstechnologie sind äußerst vielfältig. Entsprechend ist eine genaue Bezeichnung der Akteure in diesem Feld nur unzureichend mit einem Begriff erfasst. Sowohl die Unternehmensgrößen als auch die angebotenen Dienstleistungen – von Infrastruktur über Hard- und Software zu Wartungs- und Unterstützungsleistungen – variieren stark und spiegeln einen äußerst heterogenen Bereich wider. Entsprechend wurde in dieser Studie der Heterogenität des IT-Dienstleistermarktes Rechnung getragen und ein breiter Ansatz gewählt, um diese Vielfalt abbilden zu können.

Somit kommt IT-Dienstleistern nicht nur eine Schlüsselrolle im Rahmen der von KMU beanspruchten IT-Services zu, sondern ebenso bei der Umsetzung von ergänzenden IT-Sicherheitsmaßnahmen. Die Auswirkungen der Covid-19 Pandemie auf die Digitalisierungsprozesse und den damit einhergehenden IT-Sicherheitsmaßnahmen werden erst in einiger Zeit sichtbar werden. Es ist naheliegend, dass der Digitalisierungsprozess in vielen KMU, durch die Mobilitätseinschränkungen und die umfangreichen *Home-Office* Vorgaben, an Fahrt aufgenommen hat. Gleichzeitig werden sich die wirtschaftlichen Folgen der Pandemie auch auf die Investitionstätigkeiten der KMU in IT-Sicherheitsmaßnahmen auswirken und zunehmende Schwachstellen durch den steigenden Grad der Digitalisierung nur langsam oder nur unzureichend schließen. Vermutlich wird es eine kurzfristige Verschärfung der knappen fachlichen Ressourcen in der Informationstechnik geben, da die Ausbildungs- und Weiterbildungssituation der zunehmenden Digitalisierungsgeschwindigkeit hinterherhinkt.

Da es zwar Studien zur IT-Sicherheit bei KMU, aber noch keine aussagekräftigen Analysen, Befragungen oder Studien zur Rolle von IT-Dienstleistern als Akteure und Multiplikatoren für die Cybersicherheit von KMU gibt, verfolgt diese Studie das Ziel, diese Lücke zu schließen.

In der Studie werden Empfehlungen erarbeitet, wie der Beitrag der IT-Dienstleister zum Schutz der digitalen Prozesse von KMU gestärkt werden kann, um das IT-Sicherheitsniveau anzuheben. Zur Erreichung dieses Ziels wurden sowohl Anbieter von IT-Dienstleistungen, als auch die KMU als Nachfrager dieser Dienstleistungen, zunächst mithilfe von Interviews und anschließend online befragt. Bei der Befragung wurde darauf geachtet, dass sowohl die unterschiedlichen Regionen als auch die verschiedenen Wirtschaftssektoren in ihrer Breite vertreten sind. Ebenso wurde (als KMU-Definition) auf Unternehmen mit maximal 499 MitarbeiterInnen als Zielgruppe besonders eingegangen. Die Gruppe der IT-Dienstleister wurde über Verbände, Kammern und Netzwerke direkt angesprochen. Die Heterogenität dieser Dienstleistungssparte spiegelt sich in der vorgenommenen Erfassung der Multiplikatoren zur Verteilung des Online-Befragungslinks zur quantitativen Befragung der IT-Dienstleister wider.

Die Marktbetrachtung sowie die Analyse der Interviews (qualitative Befragung) und der Onlineumfragen (quantitative Befragung) der IT-Dienstleister und der KMU, die wesentliche Bestandteile dieser Studie sind, haben zahlreiche Hinweise ergeben, deren Umsetzung das Niveau der IT-Sicherheit bei KMU erhöhen würden.

- IT-Sicherheitsmaßnahmen sind ein Ergebnis von Bedrohungsanalyse und Risikobewertung. Viele KMU kennen weder ausreichend ihr Risikoprofil noch ihre individuelle Bedrohungslage. Sie unterschätzen somit häufig das Risiko, Opfer eines Angriffs zu werden. Für eine Lageeinschätzung sind zum einen für KMU und deren IT-Dienstleister gefilterte Informationen notwendig, die ein holistisches Bild der Bedrohungslandschaft zeichnen. Zum anderen müssen beide befähigt werden, eine verbesserte Selbsteinschätzung der individuellen Bedrohung vornehmen zu können. Ein Baustein des Risikomanagements kann der Abschluss von Cyberpolicen sein, da sie einerseits das betriebswirtschaftliche Risiko (teilweise) transferieren und KMU sich andererseits vor Abschluss mit den organisatorischen und technischen IT-Sicherheitsrisiken auseinandersetzen müssen.

- Im Ereignisfall wissen KMU oftmals nicht, an wen sie sich wenden können, um fachlich versierte Hilfe zu erhalten. Im Gegensatz zu Einbrüchen in der analogen Welt, ist der digitale Schaden für viele KMU nicht immer und nicht unmittelbar ersichtlich. Die Hemmschwelle, Vorfälle und Angriffe an die Polizei, die Landeskriminalämter oder andere behördlichen Stellen zu melden, ist hoch. Der Aufbau einer bundesweiten Notfall-Hotline für IT-Vorfälle mit zentraler Erreichbarkeit zur Vermittlung an regionale Ansprechstellen, würde Abhilfe schaffen. Selbiges gilt bei der Prävention durch staatlich geförderte IT-Sicherheitsförderprogramme. Für viele KMU ist der Suchaufwand, gepaart mit einer adäquaten Bedarfsanalyse, prohibitiv hoch. Eine zentrale Anlaufstelle für Förderprogramme, die KMU informiert und entsprechend vermittelt aber auch den IT-Dienstleistern für ihre KMU-Kunden zur Verfügung steht, würde

die Transparenz der Förderlandschaft erhöhen und Transaktionskosten senken. Die erst kürzlich geschaffene „Transferstelle IT-Sicherheit im Mittelstand“ (TISiM) kann an dieser Stelle Abhilfe schaffen.

- IT-Sicherheit stellt besondere Anforderungen an die fachliche Qualifikation von MitarbeiterInnen und Führungskräften. Viele IT-Sicherheitsvorfälle ließen sich mit entsprechenden IT-Sicherheitsschulungen, Trainings und regelmäßigen Auffrischungskursen vermeiden. Die Bündelung vorhandener Awareness-Plattformen durch staatliche Stellen kann Suchkosten verringern und zu mehr Akzeptanz bei KMU führen. Denkbar ist auch, eine verpflichtende Beratung in IT-Sicherheitsfragen bei Inanspruchnahme von Förderprogrammen zur Digitalisierung einzuführen.

Bei der Auswahl der IT-Dienstleister sind Nähe, wirtschaftliche Aspekte und Bekanntheit durch persönliche Netzwerke häufig entscheidende Faktoren. Qualitätskriterien sowie die Vertrauenswürdigkeit kommen weniger ausgeprägt zum Tragen. Dies liegt auch daran, dass Angebote nur schwer miteinander verglichen werden können und einheitliche Qualitätsstandards nicht existieren. Die Schaffung von Anbieterverzeichnissen mit definierten Qualitätskriterien, in denen auch Sachverständige zu IT-Sicherheit aufgelistet sind, würde zu einer besseren Transparenz und zu einem verbesserten *Matching* zwischen IT-Dienstleistern und KMU führen. KMU-spezifische IT-Sicherheitsstandards- und -zertifizierungen helfen dabei die Informationssicherheit fortlaufend zu optimieren und erhöhen das Bewusstsein der Mitarbeiter für den professionellen Umgang mit der Informationstechnik und mit schützenswerten Daten. Die weitere Etablierung von existierenden Standards für KMU und die Prüfung von möglichen Gruppenzertifizierungen zur IT-Sicherheit von KMU sollte ausgebaut werden. Dies muss unter Berücksichtigung von vertretbarem Aufwand und Kosten solcher Maßnahmen für die KMU geschehen.

Da sowohl IT-Dienstleister als auch KMU in Verbänden und Netzwerken Mitglied sind, gilt es, diese Strukturen zu nutzen, um die Bekanntheit und Akzeptanz der vorgeschlagenen Maßnahmen zu erhöhen und eine Rückkopplung zur Optimierung zu gewährleisten. Die vorliegenden Handlungsempfehlungen sind nicht statisch, sondern bedürfen einer permanenten Überprüfung und Weiterentwicklung. Die meisten Maßnahmenempfehlungen sind unseres Erachtens mit vertretbaren finanziellen und organisatorischen Ressourcen umsetzbar, und würden sowohl für die KMU, die IT-Dienstleister als auch letztlich für die Volkswirtschaft einen Mehrwert bedeuten. Die Umsetzung dieser Maßnahmen muss als eine gemeinsame Kraftanstrengung von Staat und Privatwirtschaft verstanden werden.

Die Schaffung eines übergeordneten Informationsaustausches über aktuelle Bedrohungsquellen für KMU (Lagebild) sowie geeigneter technischer und organisatorischer Schutzmaßnahmen zu deren Eindämmung, gehören zu den zentralen Aufgaben. Eine wiederkehrende Veranstaltung für IT-Dienstleister und KMU mit eigener IT-Abteilung wäre dazu erstrebenswert, in der diese Stakeholder mit Behörden und Unternehmen der IT-Sicherheit, Versicherern und Anbietern von Systemsoftware zusammengebracht werden. Auf dieser Grundlage kann ein verbesserter Informationsaustausch niedrigschwelliger ermöglicht werden und zur Netzwerkbildung beitragen. Der Fokus der Veranstaltung sollte auf dem Schwerpunkt dieser Studie liegen und insbesondere die Rolle von IT-Dienstleistern als Akteure für mehr IT-Sicherheit bei KMU berücksichtigen.

Den IT-Dienstleistern kommt eine „Gatekeeper“-Funktion zu, da sie oftmals der erste Ansprechpartner für KMU sind, wenn es um Informationen zu vertrauenswürdigen Soft- und Hardwareprodukten bzw. Servicedienstleistungen geht. Dieser Umstand muss sowohl den IT-Dienstleistern als auch den KMU deutlicher vermittelt werden. Während es den KMU häufig an Verständnis, Zeit und Budget fehlt, sich mit IT-Sicherheit intensiver auseinanderzusetzen, haben IT-Dienstleister oftmals schon volle Auftragsbücher und ein eingeschränktes Interesse an kleinteiligen Auftragsvolumen, komplizierten Entscheidungsstrukturen und einem hohen Aufwand für individuelle Leistungen, die selten skalierbar sind. Diese Diskrepanz führt u.a. zu einer wenig kosteneffizienten und qualitativ unzureichenden IT-Sicherheit bei KMU durch IT-Dienstleister.

Vor diesem Hintergrund muss die Wahrnehmung der Rolle der IT-Dienstleister als „Gatekeeper“ für die IT-Sicherheit bei KMU geschärft werden, da sie einen umfänglichen Überblick über die IT-Sicherheitslage bei KMU haben. Zugleich müssen KMU dabei unterstützt werden, IT-Dienstleister auf Fördermöglichkeiten – z.B. durch zentrale Informationsstellen – aufmerksam zu machen, um somit u.a. einen Teil der Kosten decken und die Auftragsvergabe attraktiver gestalten zu können.

Die beschriebenen Herausforderungen sollten nicht als eine rein staatliche Aufgabe verstanden werden. Privatwirtschaft und Staat müssen in eine Symbiose treten. Während die Strafverfolgung eine staatliche Aufgabe bleibt, gehört die Prävention und Schadensbegrenzung zu den gemeinschaftlichen Aufgaben. Staatliche Stellen können eine Hilfestellung bei der Bedarfsermittlung der IT-Sicherheit leisten, allerdings sind konkrete Maßnahmen von der Privatwirtschaft umzusetzen und zu bezahlen. Gleiches gilt bei der Schadensbegrenzung von Cybervorfällen. Die Aufklärung durch z.B. staatliche Stellen wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder regionale Einrichtungen wie z.B. die Digitalagenturen der Länder, fallen in den staatlichen Aufgabenbereich. Die Umsetzung jedoch ist eine private Aufgabe und schließt IT-Dienstleister, die nah an den KMU dran sind, unbedingt mit ein.

Die Umsetzung der mit der vorliegenden Studie erarbeiteten Empfehlung werden IT-Dienstleister besser unterstützen, eine stärkere Rolle bei der IT-Sicherheit ihrer KMU-Kunden einzunehmen. Die Handlungsempfehlungen sollten mit den Netzwerken der KMU und der IT-Dienstleister sowie den entsprechenden Behörden in Bund und Ländern erörtert und umgesetzt werden. Nur gemeinsam kann eine Durchdringung des KMU-Marktes erreicht werden, die alle Stakeholder einschließt, und die IT-Sicherheit aller Bereiche der Wertschöpfungskette stärkt.

2. Aufbau des Dokuments

Dieses Dokument enthält die Ergebnisse der **Studie IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland** und ist in 12 Kapitel gegliedert:

Das Kapitel **1** ist die Executive Summary, in der die wesentlichen Studienerkenntnisse kurz resümiert werden.

Der Aufbau dieses Dokuments wird im Kapitel **2** veranschaulicht.

In Kapitel **3** werden die Ausgangssituation sowie die Ziele der Studie dargelegt.

Kapitel **4** erläutert die Methodik und enthält eine detaillierte Beschreibung des Aufbaus sowie der Durchführung der Studie.

Das Kapitel **5** greift in der Marktbetrachtung die aktuelle IST-Situation des IT-Sicherheitsmarktes für KMU in Deutschland auf. Es folgt eine ausführliche Betrachtung der Angebotsseite durch die IT-Dienstleister sowie der Nachfrageseite durch die KMU auf dem deutschen IT-Sicherheitsmarkt.

In Kapitel **6** werden die Ergebnisse aus Kapitel 5 aufgenommen und als Grundlage für die Befragung der IT-Dienstleister herangezogen. Zunächst erfolgt die Festlegung der Stichprobengröße und anschließend die Erarbeitung eines Interviewleitfadens. Es folgt die qualitative Befragung von 25 IT-Dienstleistern, deren Befragungsergebnisse für die Erstellung eines quantitativen Online-Fragebogens dienen.

In Kapitel **7** folgen die Präsentation und Zusammenfassung der Studienergebnisse aus der Befragung der IT-Dienstleister. Wesentliche Erkenntnisse aus der qualitativen und quantitativen Befragung werden dargestellt.

Für die Befragung der KMU in Kapitel **8** werden ebenfalls die Ergebnisse aus Kapitel 5 herangezogen. Auch hier werden zunächst die Festlegung der geeigneten Samplegröße und die anschließende Erarbeitung eines Interviewleitfadens erläutert. Anschließend folgt die qualitative Befragung von 50 KMU. Die Befragungsergebnisse dienen der Generierung des Online-Fragebogens zur weiteren quantitativen Befragung.

In Kapitel **9** folgen die Präsentation und Zusammenfassung der Studienergebnisse aus der Befragung der KMU und eine Zusammenfassung der wesentlichen Erkenntnisse dieser Befragungen.

Das Kapitel **10** präsentiert die Handlungsempfehlungen, die sich aus den Studienergebnissen und Analysen der IT-Dienstleister sowie der KMU in den Kapitel 7 und 9 herleiten lassen.

In Kapitel **11** befindet sich der Anhang, dem alle zugrundeliegenden Dokumente und Informationen zu entnehmen sind. Im abschließenden Kapitel **12** ist das Literaturverzeichnis einsehbar.

3. Ausgangssituation und Ziele der Studie

Das Konsortium und Studienteam, bestehend aus der Neuen Köhler Managementgesellschaft (NKMG) und dem Brandenburgischen Institut für Gesellschaft und Sicherheit (BIGS), wurde vom BMWi im September 2019 beauftragt, eine Studie zum Thema „IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland“ durchzuführen. Auf Grundlage des Untersuchungsgegenstandes dieser Studie wurde zunächst die aktuelle Struktur des IT-Sicherheitsmarktes in Deutschland erörtert. Anschließend wurden relevante Themenbereiche identifiziert und Fragestellungen abgeleitet. Diese dienten als Ausgangspunkt für die Bearbeitung der Marktbetrachtung und die anschließende qualitative und quantitative Befragung der IT-Dienstleister und der KMU.

Die Analyse fokussierte sich dabei auf die Untersuchung des bestehenden IT-Sicherheitsniveaus von KMU in Deutschland. Dazu erfolgte zunächst eine Marktbetrachtung. Das Studienteam untersuchte hierfür bereits bestehende Analysen und Studien. Es folgten deutschlandweit branchenübergreifende qualitative, persönliche Interviews mit 25 ausgewählten IT-Dienstleistern und 50 ausgewählten KMU, deren anonymisierte Ergebnisse als Basis für die quantitativen Online-Befragungen weiterer IT-Dienstleister und KMU dienten. Die Zielgröße der Online-Befragungen lag sowohl auf der Angebots- als auch auf der Nachfrageseite bei 100 Unternehmen. Diese Zielgröße konnte bei der Online-Befragung der KMU nicht ganz erreicht werden.

Da das Thema IT-Sicherheit unterschiedliche Geschäftsprozesse der KMU betrifft, wurden im Rahmen der Studie technische, organisatorische, personelle, infrastrukturelle, anwendungsbezogene sowie managementbezogene und präventive Aspekte analysiert. Um einen möglichst umfassenden Überblick über die IST-Situation der IT-Sicherheit von KMU in Deutschland zu erhalten und potentiellen Handlungsbedarf zu erkennen, wurden bei den Befragungen sowohl die Angebotsseite der IT-Dienstleister als auch die Nachfrageseite der KMU betrachtet. Zudem wurden die unterschiedlichen Unternehmensebenen (Geschäftsführung, IT-Abteilung, Marketingabteilung) berücksichtigt.

Ziel der Auftragsstudie ist die Untersuchung und Darstellung eines aktuellen Lagebilds der IT-Sicherheit bei KMU in Deutschland mit Bezug zur Angebots- und Nachfrageseite von IT-Dienstleistungen. Dazu wurden zunächst die IT-Dienstleister sowie anschließend die KMU befragt und deren Befragungsergebnisse analysiert und ausgewertet.

Folgende Fragestellungen sollten mithilfe von qualitativen und quantitativen Befragungen beantwortet werden:

IT-Dienstleister (Angebotsseite)	KMU (Nachfrageseite)
➢ Wie schätzen IT-Dienstleister die Bedrohungslage bei KMU bezüglich IT-Sicherheitsrisiken ein? Gibt es Optimierungsbedarf?	➢ Wie schätzen KMU die eigene Bedrohungslage bezüglich IT-Sicherheitsrisiken ein? Wie sind KMU im Punkt IT-Sicherheit aufgestellt? Gibt es etablierte Sicherheitsstrategien und -prozesse? Wer verantwortet IT-Sicherheit? Gibt es Optimierungsbedarf?
➢ Wie informieren sich IT-Dienstleister über aktuelle IT-Sicherheitsvorfälle?	➢ Wie und wie häufig informieren sich KMU über aktuelle IT-Sicherheitsvorfälle und wie gehen sie mit Cyber-Bedrohungen um? Sind sich KMU der verschiedenen Sicherheitsrisiken bewusst und wie schätzen sie das eigene Risiko ein?
➢ Wie arbeiten IT-Dienstleister mit KMU unter der Fragestellung der IT-Sicherheit zusammen? Gibt es ein spezifisches Leistungsportfolio für KMU?	➢ Gibt es etablierte Regelungen und Prozesse zum Thema IT-Sicherheit bei KMU?
➢ Welche Multiplikatoren existieren im Bereich der IT-Dienstleister für KMU?	➢ Wie hoch ist das Budget für IT-Sicherheit?
➢ Sind IT-Dienstleister in Verbänden oder Netzwerken organisiert?	➢ Spielt Outsourcing beim Thema IT-Sicherheit für KMU eine Rolle? Was und wie oft wird outgesourct? Und haben KMU diesbezüglich irgendwelche Bedenken?
➢ Gibt es auf der Nachfrageseite regionale Unterschiede?	➢ Gibt es auf der Anbieterseite regionale Unterschiede? Gibt es in den Größenklassen von Kleinst-, Klein- und Mittlere Unternehmen Unterschiede bezüglich der Anforderungen oder Risiken?
➢ Über welche Expertisen verfügen die MitarbeiterInnen der IT-Dienstleister standardmäßig und welche Aspekte sind relevant? Spielt Weiterbildung eine Rolle?	➢ Gibt es Aspekte, die die Zusammenarbeit mit IT-Dienstleistern erschweren oder gar verhindern?

➢ Wie erfolgt die Neukundenakquisition im Kundensegment der KMU? Ist Wachstum im Kundensegment der KMU für IT-Dienstleister interessant? Gibt es Hemmnisse in der Zusammenarbeit mit KMU?	➢ Wie und nach welchen Auswahlkriterien finden KMU geeignete IT-Dienstleister? Welche Qualitätsanforderungen und Standards sind für KMU bei der Auswahl geeigneter IT-Dienstleister relevant?
➢ Welche Leistungen werden von den Kunden besonders häufig angefragt?	➢ Entspricht das Produktportfolio der IT-Dienstleister den Bedürfnissen der KMU?
➢ Sind den IT-Dienstleistern staatliche Fördermaßnahmen bekannt? Gibt es Optimierungspotential? Welche Fördermaßnahmen wären wünschenswert?	➢ Sind den KMU die staatlichen Fördermaßnahmen bezüglich IT-Sicherheit bekannt und nehmen sie diese in Anspruch? Gibt es Optimierungspotential? Welche Fördermaßnahmen wären wünschenswert?

Der abschließende Teil der Studie enthält Handlungsempfehlungen, die aus den Ergebnissen der Befragungen gewonnen werden konnten. Diese Handlungsempfehlungen sollen dazu dienen, das Bewusstsein für IT-Sicherheit weiter zu stärken, das Portfolio der IT-Dienstleister zielgerichtet auf die Bedürfnisse der KMU auszurichten und den KMU bedarfsgerechte Angebote zur Verfügung zu stellen.

Die Studienergebnisse sollen dazu beitragen, das aktuelle IT-Sicherheitsniveau von KMU unter Einbindung von IT-Dienstleistern in Deutschland transparenter zu gestalten. Zudem sollen die Handlungsempfehlungen der Verbesserung des IT-Sicherheitsniveaus dienen.

Die Studie wurde im Zeitraum vom 1. November 2019 bis zum 16. November 2020 durchgeführt. Der Projektplan umfasste die folgenden fünf Projektphasen:

- Marktbetrachtungen / Aktueller Stand
- Qualitative und quantitative Befragung der IT-Dienstleister
- Qualitative und quantitative Befragung der KMU
- Erstellung der Studienergebnisse
- Studienpräsentation

4. Methodik

Um die Erfüllung des Untersuchungsgegenstandes zu gewährleisten, wurden für die ersten drei Projektphasen eine eigene, auf die jeweilige Phase abgestimmte Methodik gewählt. Für die Marktbetrachtung griff das Konsortium auf Wunsch des BMWi auf Sekundärliteratur zurück und wertete umfangreiche nationale sowie internationale Studien aus.

Die Methodik des theoretischen Sampling für die Festlegung der Interviewstichproben für die **qualitative Befragung der IT-Dienstleister und der KMU** wird in den folgenden Abschnitten erläutert.

Aus den Interviewergebnissen der IT-Dienstleister und der KMU-Befragung wurde der erarbeitete Interviewleitfaden weiterentwickelt und in die Fragestellungen des Online-Befragungstools überführt. Die Online-Befragung erfolgte mithilfe des Tools SoSciSurvey. Die Online-Befragung der IT-Dienstleister und der KMU erfolgte über Verteilung des bereitgestellten Befragungslinks an die jeweiligen Zielgruppen.

Die Analyseergebnisse wurden in fünf Handlungsfelder und ein querschnittliches Handlungsfeld gruppiert. Ziele und Maßnahmenvorschläge sind handlungsfeldgenau erarbeitet worden.

4.1. Sampling-Methodik und Stichprobe für die IT-Dienstleister

Für die qualitative Befragung der IT-Dienstleister wurde zunächst ein theoretisches Sampling erstellt. Mithilfe des theoretischen Samplings, welches der qualitativen Sozialforschung zugeordnet ist, können komplexe Fragestellungen auf eine heterogene Untersuchungsgruppe angewandt werden, ohne dabei relevante Informationen zu verlieren. Beim theoretischen Sampling wird zunächst ein Untersuchungsrahmen bestimmt, der einen typischen Untersuchungsfall darstellt und konkrete Kriterien festlegt. Das ermöglicht eine Varianzmaximierung, die Erweiterung der Informationsbasis, indem die ermittelten Informationen zu Annahmen verdichtet und entsprechende Hypothesen aufgestellt werden. Diese Vorgehensweise ermöglicht darüber hinaus in eingeschränktem Maße Schlussfolgerungen, die auf die Gesamtheit des Untersuchungsgegenstandes übertragen werden können.

Für die weitere Untersuchung wurden zunächst IT-Dienstleister definitorisch eingegrenzt (siehe Abschnitt 5.3.1). Das Statistische Bundesamt zählt zu den Aufgaben von IT-Dienstleistern „z. B. Anpassung, Testen und Pflege von Software, Planung und Entwurf von Computersystemen, die Hardware, Software- und Kommunikationstechnologie umfassen, Verwaltung und Betrieb der Computersysteme und Datenverarbeitungsanlagen eines Kunden vor Ort sowie sonstige

fachliche und technische mit der Datenverarbeitung verbundene Tätigkeiten."[1] Unternehmen, die Informationsdienstleistungen wie z.B. Datenverarbeitung und andere Tätigkeiten zur Erstellung von Informationen erbringen, sind davon abzugrenzen.[2]

Darüber hinaus können weitere Abgrenzungen, wie z.B. in den jährlich erscheinenden *Lünendonk*-Studien zum Markt für IT-Beratungen und IT-Services, vorgenommen werden. In der *Lünendonk*-Studie 2019, die für die Marktbetrachtung in Kapitel 5 analysiert wurde, wird zwischen IT-Beratungs- und Systemintegrationsunternehmen einerseits, die mehr als 60% ihres Umsatzes mit Change-the-Business-Leistungen (IT-Beratung, Entwicklung von Individualsoftware, etc.) erwirtschaften, und IT-Service/-Dienstleistern andererseits, deren Tätigkeiten sich hauptsächlich um Wartungs- und Unterstützungsleistungen (support) sowie um den Betrieb der Anwendungsumgebungen und Rechenzentren drehen, unterschieden.[3] Nachfolgend werden all diese Tätigkeiten unter dem Sammelbegriff der IT-Dienstleister zusammengefasst und decken somit ein breites Spektrum an Unternehmen und Dienstleistungen ab, die sich in den qualitativen und quantitativen Umfragen ebenso wiederfinden.

Die in dieser Studie angewandten Sampling-Kriterien der befragten IT-Dienstleister sind die Unternehmensgröße und die Region. Beim Größenkriterium orientiert sich diese Studie an der KMU-Definition des Instituts für Mittelstandsforschung (IfM) Bonn,[4] siehe Tabelle 1.

Tabelle 1 Unternehmensgröße gemäß der KMU-Definition des Instituts für Mittelstandsforschung (IfM) Bonn

Unternehmensgröße	Beschäftigtenzahl
Kleinstunternehmen	Bis zu 9 MitarbeiterInnen
Kleinunternehmen	Zwischen 10 – 49 MitarbeiterInnen
Mittlere Unternehmen	Zwischen 50 und 499 MitarbeiterInnen

Hierbei wurden die IT-Dienstleister in die Kategorien »Kleinstunternehmen« [bis zu 9 MitarbeiterInnen], »Kleinunternehmen« [bis zu 49 MitarbeiterInnen] und »mittlere Unternehmen« [bis zu 499 MitarbeiterInnen] eingeteilt. Zusätzlich erfolgte eine regionale Einteilung in die Bereiche »West Ballung«, »West Land«, »Ost Ballung« und »Ost Land«.

[1] Vgl. Destatis 2019, 7.
[2] Ebd.
[3] Vgl. Lünendonk 2019, 5.
[4] Siehe https://www.ifm-bonn.org/definitionen-/kmu-definition-des-ifm-bonn

Daraus ergab sich die in Tabelle 2 dargestellte Sampling-Matrix, aus der sich 3x2x2 = 12 verschiedene Sets ergaben, in denen pro Kategorie die Befragung von jeweils zwei Unternehmen vorgesehen war. Somit ergab sich inklusive eines durchgeführten Pretests eine Gesamtstichprobe von insgesamt 25 zu befragenden IT-Dienstleistern:

Tabelle 2 Sampling-Matrix der IT-Dienstleister nach Größe und Region für die qualitative Befragung

	Kleinstunternehmen [bis 9 MitarbeiterInnen]	Kleinunternehmen [bis 49 MitarbeiterInnen]	Mittlere Unternehmen [bis 499 MitarbeiterInnen]
Ost Ballungsraum	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2
Ost Land	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2
West Ballungsraum	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2
West Land	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2	Unternehmen 1 Unternehmen 2

Die Auswahl geeigneter InterviewpartnerInnen für die qualitative Befragung der IT-Dienstleister (siehe Abschnitt 6.2) erfolgte auf Basis der zuvor beschriebenen Sampling-Matrix. Bei der Ansprache der IT-Dienstleister wurde das Konsortium durch ein Begleitschreiben des BMWi unterstütz (siehe 11.5 im Anhang). Die InterviewpartnerInnen wurden vom Konsortium persönlich recherchiert und befragt. Während die Befragungen zunächst vor Ort, in den jeweiligen Geschäftsräumen der InterviewpartnerInnen durchgeführt wurden, erfolgten die Interviews ab dem 14.03.2020, aufgrund der aktuellen COVID-19-Pandemie, ausschließlich telefonisch oder via Videocalls bzw. -konferenz.

Die quantitative Befragung der IT-Dienstleister (siehe Abschnitt 6.4) wurde mittels eines Online-Fragebogens[5] durchgeführt. Die Verteilung des Befragungslinks erfolgte durch das Konsortium selbst sowie über die im Abschnitt 6.4 aufgeführten Multiplikatoren.

Ein vollständiges Clipping zur Veröffentlichung des Befragungslinks ist dem Anhang (siehe PDF Anhang) zu entnehmen.

Bei der quantitativen Befragung der IT-Dienstleister wurde das Konsortium ebenfalls durch ein Begleitschreiben des BMWi unterstützt (siehe 11.6 im Anhang).

[5] Eine Druckansicht des quantitativen Online-Fragebogens für die IT-Dienstleister ist dem Anhang zu entnehmen.

4.2. Sampling-Methodik und Stichprobe für die KMU

Für die qualitative Befragung der KMU wurde auch das zuvor beschriebene theoretische Sampling (siehe Abschnitt 4.1) verwendet. Die Sampling-Kriterien der KMU waren die Unternehmensgröße (siehe Tabelle 1) und der Wirtschaftsbereich (siehe Tabelle 3), entsprechend der Definition des Instituts für Mittelstandsforschung (IfM) Bonn.

Tabelle 3 Wirtschaftsbereiche gemäß der Definition des Instituts für Mittelstandsforschung (IfM) Bonn

Wirtschaftsbereiche gemäß der Definition des Instituts für Mittelstandsforschung (IfM) Bonn	
verarbeitendes Gewerbe	Verkehr, Information und Kommunikation
Bergbau, Energie, Ver- und Entsorgung	Finanzen, Versicherungen, Grundstücks- und Wohnungswesen
Baugewerbe	unternehmensnahe Dienstleistungen
Handel und Gastgewerbe	personenbezogene Dienstleistungen

Die Auswahl der zu befragenden KMU erfolgte aus den Wirtschaftsbereichen »verarbeitendes Gewerbe«, »Bergbau, Energie, Ver- und Entsorgung«, »Baugewerbe«, »Handel und Gastgewerbe«, »Verkehr, Information und Kommunikation«, »Finanzen, Versicherungen, Grundstücks- und Wohnungswesen«, »unternehmensnahe Dienstleistungen« und »personenbezogene Dienstleistungen«.

Aus den Sampling-Kriterien Wirtschaftsbereich und Größe ergab sich somit folgende, in der Tabelle 4 dargestellte Sampling-Matrix, in der pro Kategorie die Befragung von jeweils zwei Unternehmen vorgesehen war. Für die qualitative Befragung der KMU (siehe Kapitel 8.2) ergab sich folglich eine Stichprobe von 8x3x2 = 48 zu befragenden Unternehmen, zuzüglich zwei weiterer, ursprünglich als Pretest vorgesehene Unternehmen. Somit beläuft sich die Zahl der Stichproben auf 50:

Tabelle 4 Sampling-Matrix der KMU nach Größe und Wirtschaftsbereich für die qualitative Befragung

Wirtschaftsbereich	Kleinstunternehmen [bis 9 MitarbeiterInnen]	Kleinunternehmen [bis 49 MitarbeiterInnen]	Mittlere Unternehmen [bis 499 MitarbeiterInnen]
Baugewerbe	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2

Bergbau, Energie-, Wasserversorgung, Entsorgung	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2
Finanz-/Versicherungs-dienstleistungen, Grundstücks- und Wohnungswesen	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2
Handel, Gastgewerbe	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2
Personenbezogene Dienstleistungen	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2
Unternehmensnahe Dienstleistungen	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2
Verarbeitendes Gewerbe	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2
Verkehr, Information und Kommunikation	Unternehmen 1	Unternehmen 1	Unternehmen 1
	Unternehmen 2	Unternehmen 2	Unternehmen 2

Es folgte die Erstellung eines Interviewleitfadens für die qualitative Befragung (siehe PDF Anhang). Diese Interviews wurden aufgrund der aktuellen COVID-19-Pandemie ausschließlich telefonisch durchgeführt. Die Ergebnisse der qualitativen Befragungen dienten als Grundlage für die Erstellung des Online-Fragebogens[6] für die quantitative Befragung der KMU. Der Online-Fragebogen wurde zusammen mit einem Begleitschreiben (siehe 11.7 im Anhang) des BMWi u.a. über die Projektseite der NKMG[7] veröffentlicht. Zudem wurde die Online-Befragung der KMU durch MultiplikatorInnen beworben und verteilt (siehe Tabelle 7).

[6] Eine Druckansicht des quantitativen Online-Fragebogens für die KMU ist dem Anhang zu entnehmen.
[7] Veröffentlichung des Befragungslinks des KMU-Fragebogens über die Projektseite der NKMG, https://www.nkmg-berlin.de/projekte/befragung-zur-studie-it-sicherheit-des-bmwi/kmu-befragung

5. Marktbetrachtung

Die vorliegende Marktbetrachtung soll einen Überblick der relevanten Literatur mit Bezug zur Angebots- und Nachfrageseite von IT-Dienstleistungen unter besonderer Berücksichtigung der IT-Sicherheit geben. Auf der Nachfrageseite werden explizit nur kleine und mittlere Unternehmen (KMU) berücksichtigt.[8] KMU spielen eine zentrale Rolle für die Wirtschaftskraft der Bundesrepublik Deutschland und stehen u.a. durch die zunehmende Digitalisierung und Vernetzung der gesamten Wertschöpfungskette unter einem transformativen Druck, der sich auch auf die Sicherheits- und Schutzleistungen auswirkt. IT- und Cybersicherheit sind ein wesentlicher Teil der Sicherheits- und Schutzleistung von Unternehmen. Laut BSI umfasst der Begriff der Cybersicherheit alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik und geht somit über das Aktionsfeld der klassischen IT-Sicherheit hinaus. Eingeschlossen sind Prozesse, Anwendungen und Kommunikation, welche mithilfe von Informationstechnik verarbeitet werden, die an das Internet oder vergleichbare Netze gekoppelt ist.[9]

Aufgrund ihrer geringen Größe sowie fehlender eigener Kompetenz und Ressourcen ist eine Vielzahl von KMU bei Themen rund um Digitalisierung regelmäßig auf die Hilfe externer IT-Dienstleister angewiesen. Diese sind oftmals die ersten Ansprechpartner, wenn KMU sich mit Fragen der IT-Sicherheit auseinandersetzen (müssen). Zwar gibt es innerhalb des Segments der IT-Dienstleister Unternehmen, die sich auf IT-/Cybersicherheit spezialisiert haben, gleichwohl werden diese als erster Ansprechpartner entweder erst im konkreten Bedrohungs- oder Schadensfall, zumeist über den generellen IT-Dienstleister eines Unternehmens, hinzugezogen, oder ihr Kunde ist selbst in einem besonders bedrohten Marktumfeld aktiv, welches die Dienstleistungen eines Cybersicherheitsunternehmens notwendig macht.[10]

In der folgenden Marktbetrachtung soll die Rolle der IT-Dienstleister für die IT-Sicherheit von KMU in Deutschland untersucht werden. Da insbesondere KMU für die digitale Transformation, aber auch für den Schutz der eigenen Infrastruktur, Informationstechnik, IT-Systeme und des Know-hows, sowie der Wertschöpfungskette, auf die Kenntnisse und Erfahrungen externer IT-Dienstleister angewiesen sind, kommt letzteren eine Schlüsselrolle zu. Fehlendes Know-how wird eingekauft, lokale Datenbanken werden in Clouds transferiert und mit anderen Datenbanken konsolidiert und Altsysteme werden in neue Software transformiert. Zudem wird alles mit den Anforderungen der IT- und Cybersicherheit kombiniert.[11] Bei all diesen Prozessen benötigen KMU die Unterstützung von IT-Dienstleistern.

Die Marktbetrachtung ist wie folgt gegliedert: Zunächst wird das methodische Vorgehen in Abschnitt 5.1 dargelegt. Daran anschließend wird in 5.2 die Ausgangslage, insbesondere mit Blick auf die Bedrohung im Cyberraum, für KMU betrachtet. Vor diesem Hintergrund werden relevante Akteure der Angebotsseite (IT-Dienstleister) in Abschnitt 5.3 identifiziert, um ihren Stellenwert für das Cybersicherheitsniveau von KMU in Deutschland zu untersuchen. Hierzu

[8] Wenn nicht anders kenntlich gemacht wird die KMU-Definition des Instituts für Mittelstandforschung (IfM) Bonn verwendet, www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/, Zugriff v. 14.02.2020.
[9] Vgl. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html, Zugriff v. 10.03.2020.
[10] Diese Aussagen basieren auf Erfahrungen der Autoren.
[11] Vgl. Lünendonk 2019, 7 ff.; Systemhaus 2018, 16.

werden Erkenntnisse über das Produktportfolio, die Unternehmensstruktur sowie die Wettbewerbssituation zusammengetragen, um die Marktstruktur der IT-Dienstleister in Deutschland besser einschätzen zu können. Anschließend wird in Abschnitt 5.4 auf der Nachfrageseite anhand vorhandener Quellen analysiert, wie KMU ihren IT-Dienstleister auswählen, welche Leistungen sie nachfragen und wie die Entscheidungsprozesse hierfür zustande kommen. Aus der vorangegangenen Analyse wurden in Abschnitt 5.5 Wissenslücken identifiziert, die in die folgenden qualitativen und quantitativen Umfragen der Anbieter von IT-Dienstleistungen sowie der KMU als Nachfrager, eingeflossen sind. Die identifizierten Wissenslücken werden auf Anbieterseite der IT-Dienstleister und auf Nachfragerseite der KMU, näher erörtert.

5.1. Methodisches Vorgehen

Für die Durchführung der Marktbetrachtung wurde eine umfassende Literatur- und Dokumentanalyse öffentlicher Quellen vorgenommen. Dabei wurde zwischen wissenschaftlichen Quellen und Studien von MarktteilnehmerInnen, Verbänden und Behörden unterschieden. Bei der Auswertung und Priorisierung der Quellen wurde auf das institutionelle Wissen und den Quellenbestand des Autorenteams zurückgegriffen, das zum Teil jahrzehntelange Erfahrungen auf beiden Marktseiten angesammelt hat.

Die gewonnenen Erkenntnisse wurden gegliedert in die

- **Ausgangslage**, die im Wesentlichen Definitionen sowie Informationen über die Bedrohungslage und die Schäden beinhaltet.
- **Angebotsseite**, die eine Analyse der IT-Dienstleister unter besonderer Berücksichtigung ihres Angebots an IT-Sicherheitsprodukten und Dienstleistungen umfasst.
- **Nachfrageseite**, und hier nur die Nachfrage von kleinen und mittleren Unternehmen (KMU).

Dieser Schritt dient zur Abgrenzung des zu untersuchenden Feldes sowie des Erkenntnisgewinns über die aktuelle Marktstruktur, die angebotenen IT-Sicherheitsprodukte und -dienstleistungen sowie der momentanen Umsetzungslücke hinsichtlich der IT-Sicherheit auf der Nachfrageseite.

Diese Erkenntnisse sind wichtig, um im weiteren Verlauf das Ziel der Studie, die Betrachtung von IT-Dienstleistern als Akteure, die zur Stärkung der IT-Sicherheit von KMU dienen, herauszuarbeiten. Zur Validierung und Vertiefung der so gewonnenen Ergebnisse wird in einem nächsten Schritt zunächst eine qualitative Befragung ausgewählter IT-Dienstleister durchgeführt. Dazu wird u.a. aus den gewonnenen Erkenntnissen der Marktbetrachtung, sowie identifizierter Wissenslücken, ein Interviewleitfaden erstellt, der in fünf zu validierende Bereiche unterteilt wird:

- Wahrgenommene Risiken der IT-Sicherheit von KMU
- Produktportfolio und technische Lösungen der IT-Dienstleister
- Arbeitsorganisation und -prozess der IT-Dienstleister

- Qualifikation und Weiterbildung der MitarbeiterInnen der IT-Dienstleister
- Marketingkommunikation/Neukundenakquisition

Der Marktanalyse und der qualitativen Befragung mithilfe des generierten Interviewleitfadens wird im Projekt eine quantitative Befragung der IT-Dienstleister folgen. Der Fragebogen wird aus dem Leitfaden der qualitativen Befragung und den gewonnenen Ergebnissen der durchgeführten qualitativen Befragungen abgeleitet.

Für die vorliegende Marktbetrachtung wurden neben der zitierten wissenschaftlichen Literatur weitere Studien, Strukturdaten und Publikationen analysiert (siehe Abschnitt 11.3 und 11.4).

5.2. Ausgangslage

Die fortschreitende Transformation zur digitalen Gesellschaft bietet der deutschen Wirtschaft viele Möglichkeiten, die Produktivität zu steigern sowie neue und innovative Geschäftsmodelle zu entwickeln. Kostensenkungen bzw. Effizienzsteigerungen, eine erhöhte Wettbewerbsfähigkeit und Qualitätssteigerungen werden häufig mit der Digitalisierung von Wertschöpfungsketten verfolgt. Gleichzeitig führt die zunehmende Vernetzung dazu, dass Schnittstellen zur Außenwelt geschaffen werden, die neue Angriffsvektoren für Kriminelle, Saboteure oder im staatlichen Auftrag bzw. unter Duldung staatlicher Stellen agierende Angreifer, bieten. Die Digitalisierung selbst führt also dazu, dass die Bedrohung durch Cyberangriffe zunimmt.

Datenverlust, Ausfälle der IT-Systeme sowie -Infrastrukturen oder Produktionsausfälle aufgrund von Cyberangriffen können nicht nur zu hohen Verlusten führen, sondern in Einzelfällen existenzbedrohend sein.[12] Das volkswirtschaftliche Wachstumspotenzial der Digitalisierung kann erst dann voll ausgeschöpft werden, wenn den damit einhergehenden Bedrohungen im Cyberraum angemessen begegnet wird. Auf Unternehmensebene muss das durch die Digitalisierung entstehende Cyberrisiko betriebswirtschaftlich und technisch beherrschbar werden. Dafür muss zunächst Klarheit darüber herrschen, welche Bedrohungen tatsächlich in einer Periode vorliegen (Lagebild) und zum anderen, welche Schutzmaßnahmen geeignet sind, diese wirksam zu begrenzen.

Abbildung 1 veranschaulicht das schematische Grundkonzept des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS) von Sicherheit als Funktion aus Bedrohung(en) und Schutzleistung(en). Bedrohungen aus dem Cyberraum können sowohl Unternehmen, in Form von u.a. Kriminalität, Spionage und Sabotage, sowie BürgerInnen, als auch den Staat und seine Einrichtungen treffen. Es muss eine ausgewogene Balance zwischen zweckgebundenen Schutzleistungen und zielgerichteten Maßnahmen gefunden werden, um das Bedrohungspotenzial zu reduzieren (minimieren).

[12] Vgl. BSI 2019b, 48; vgl. BSI 2020, 13.

Grundsätzlich haben Unternehmen die Möglichkeit durch eine Kombination von drei Arten von Schutzmaßnahmen Cyberbedrohungen zu begegnen und ein für sie befriedigendes Sicherheitsmaß zu erreichen:

1. Sie können mit **technischen und organisatorischen Maßnahmen** das Bedrohungspotenzial reduzieren.
2. Sie können durch Aus- und Weiterbildung des eigenen Personals oder das Einkaufen von qualifiziertem **Humankapital** die Erfolgswahrscheinlichkeit eines Angriffs reduzieren.
3. Sie können den finanziellen Schaden, der durch einen Cyberangriff entsteht, mithilfe des Risikotransfers an einen Dritten, in der Regel eine Versicherung, weiterreichen.

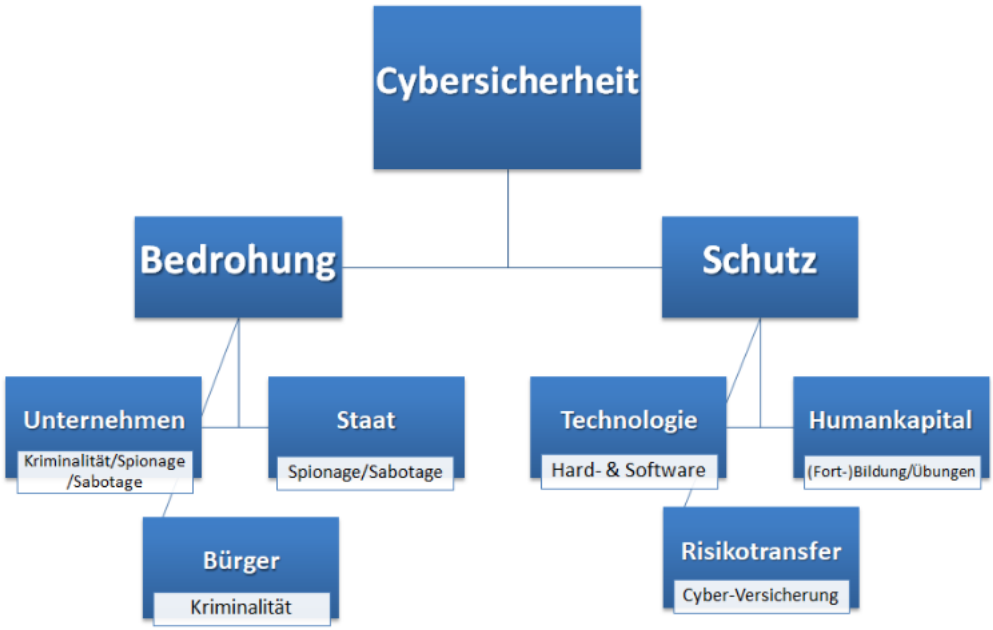

Abbildung 1 – Cybersicherheit als Funktion aus Bedrohung und Schutz, Quelle: Schematisches Konzept des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS).

Cybersicherheit ist ein äußerst dynamisches Feld, auf dem zwischen Angreifern und Verteidigern eine gewisse **Ungleichzeitigkeit** herrscht. Neue Bedrohungen durch die Entdeckung von Schwachstellen können von jetzt auf gleich entstehen. Böswillige Angreifer verändern ihre Angriffsmethode, nutzen neue Netzwerke und gehen Verbindungen mit staatlichen Akteuren ein oder bieten ihre Fähigkeiten auf dem Schwarzmarkt Dritten an. Demgegenüber ist der Schutz vor solchen Bedrohungen vergleichsweise träge. Der Umgang von Staat und Unternehmen mit neuen und derart dynamischen Herausforderungen wie der Cybersicherheit ist systembedingt durch eine gewisse zeitliche Verzögerung charakterisiert. Die Herausforderungen für KMU zur Beherrschung dieses dynamischen Felds sind einerseits bei der Analyse von eigenen Schwachstellen aber auch bei der Auswahl der geeigneten IT-Dienstleister außerordentlich hoch.

Die **Sensibilisierung** der Akteure für diese Themen ist eine notwendige Voraussetzung, um geeignet auf Cyberbedrohungen reagieren zu können. Hier sind in den letzten Jahren erhebliche Anstrengungen von staatlichen Institutionen und Unternehmensverbänden vorgenommen worden. Generell scheint sich bei einer Mehrheit der Unternehmen in Deutschland die Erkenntnis durchgesetzt zu haben, dass die Anzahl von Cyberangriffen in Zukunft eher zunehmen wird. Insgesamt glauben 82% der Unternehmen mit 10-99 MitarbeiterInnen, 78% mit 100-499 MitarbeiterInnen und 80% mit 500 oder mehr MitarbeiterInnen, dass Cyberangriffe stark oder eher zunehmen werden.[13] Das Bewusstsein allein ist bei Weitem nicht hinreichend, wenn die Chancen und Risiken z.T. erkannt werden, sich daraus aber keine konkreten Handlungen ableiten, die zu einem höheren Schutzniveau führen.

Eine verlässliche **Informationspolitik**, die Schadensfälle analysiert, kategorisiert und darauf basierend Bedrohungsszenarien anpasst, ist für die Wirksamkeit und den Einsatz von geeigneten Schutzmaßnahmen notwendig. Dabei zeichnet sich ab, dass die tatsächliche Bedrohungslage nur sehr unzureichend erfasst ist und es sich um eine unübersichtliche Gemengelage an unterschiedlichen Akteuren, Intentionen und Einschätzungen handelt.[14] Darüber hinaus sind detaillierte Informationen zu Schadensvorfällen und spezifischen Angriffsmechanismen z.T. nicht öffentlich zugänglich. Zwar werden gezielt Informationen zu aktuellen Bedrohungsquellen an einzelne entsprechende Adressaten verteilt, z.B. vom BSI an Betreiber kritischer Infrastrukturen, jedoch führt diese Praxis dazu, dass wichtige Erkenntnisse der Öffentlichkeit und auch der Wissenschaft vorenthalten werden.[15] Insbesondere die KMU stehen vor der anspruchsvollen Aufgabe, die vorhandenen Informationen und Bedrohungen zielgerichtet für das eigene Unternehmen bewerten zu müssen.

Als Folge digitaler Spionage, Sabotage und Kriminalität verzeichnete die deutsche Wirtschaft in den vergangenen beiden Jahren laut *Bitkom* **Schäden** in Höhe von etwa 100 Mrd. Euro.[16] Dies ist nahezu eine Verdoppelung der Schadenssumme des Jahres 2017 in Höhe von 55 Mrd. Euro. Viele Cyberangriffe sowie die damit verbundenen Schäden, bleiben oftmals lange Zeit unentdeckt.[17] Identifizierte Cyberangriffe werden den Sicherheitsbehörden unter Umständen nicht gemeldet.[18] In Anbetracht des Schadenumfangs erscheinen die Investitionen deutscher Unternehmen in IT-Sicherheitsdienstleistungen, zuletzt 2,1 Mrd. Euro im Jahr 2018, verhältnismäßig gering.[19]

Mithilfe anonymer Befragungen lässt sich ein besserer Eindruck über die **Schadenshäufigkeit** in Deutschland gewinnen. Im Jahr 2017 gaben ca. 70% der Unternehmen und Institutionen in der Cyber-Sicherheits-Umfrage der *Allianz für*

[13] Vgl. Bitkom 2019a, 10.
[14] Vgl. www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html, Zugriff v. 14.02.2020 und Bitkom 2018b, 5.
[15] Vgl. Bretschneider, W., Rieckmann, J., Stuchtey, T., Szanto, A. 2020, 137; & Informationen des Nationalen Cyber-Abwehrzentrums. Gefährdungslage der Stromversorgung in Deutschland durch Cyberangriffe https://fragden-staat.de/anfrage/lageeinschatzung-zu-stromnetz/104895/anhang/GefhrdungslagederStromversorgunginDeutschlanddurchCyberangriffe.pdf, Zugriff v. 14.02.2020.
[16] Vgl. Bitkom 2020b, 23. Für die Jahre 2018 und 2019 wurde ein Gesamtschaden von 205,7 Mrd. Euro errechnet.
[17] Vgl. DsiN 2018, 12.
[18] Vgl. BKA 2020, 3.
[19] Vgl. Statista 2019.

Cyber-Sicherheit an, in den vorangegangenen zwei Jahren Opfer von Cyberangriffen geworden zu sein.[20] In der letzten Cyber-Sicherheits-Umfrage gaben 26% der KMU an, 2018 von Cybersicherheits-Vorfällen betroffen gewesen zu sein.[21] Die im Vergleich zur vorherigen Erhebung geringere Zahl der Betroffenen liegt zum einen daran, dass in der letzten Umfrage genauer zwischen KMU (1 bis 249 Beschäftigte) und großen Unternehmen (mit 250 und mehr Beschäftigten) unterschieden wurde und zum anderen, dass sich der Betrachtungszeitraum auf ein Jahr erstreckte.[22]

Gleichzeitig sollte berücksichtigt werden, dass vor allem in KMU aufgrund mangelnder IT-Sicherheitsmaßnahmen zur Detektion viele Vorfälle unerkannt bleiben. Darauf deutet auch hin, dass 88% der befragten Unternehmen zwar anerkennen, dass mit der zunehmenden Digitalisierung neben den sichtbaren Chancen auch unsichtbare Risiken wachsen, aber nur 29% Cybersicherheit als einen Wettbewerbsvorteil verstehen.[23]

Insgesamt verfolgt die Mehrzahl der Cyberangriffe vor allem monetäre Interessen.[24] Cyberkriminalität ist ein boomendes Geschäft geworden. Eine signifikante Zunahme von Erpressungs-Trojaner-Kampagnen, sogenannte Ransomware, mit dem Ziel, Lösegeld für die Wiederhergabe von Unternehmensdaten zu erbeuten, war branchenübergreifend zu verzeichnen.[25] Solche Kampagnen sind derzeit für die meisten Cyber-Angriffe verantwortlich und verursachen gleichzeitig immense Kosten (sowohl direkte Kosten als auch Folgekosten).[26] Die Vorgehensweise der Angreifer ist dabei sehr dynamisch und passt sich neuen Schutzmaßnahmen schnell an.

Die Auswahl und Ausspähung bestimmter Objekte, zwecks zielgerichteter Angriffe (*Targeted Attack*), scheint allgemein zuzunehmen, während massive Angriffe auf breite Benutzersegmente (*Low Hanging Fruit*) weiterhin ein probates Mittel sind.[27]

In einer engmaschigen Wertschöpfungskette können Angriffe auf einzelne Teile der Lieferkette den kompletten Verbund gefährden und als Einfallstor dienen. Da es schwierig ist, alle Komponenten mit geeigneten Sicherheitsverfahren entlang der Kette auszustatten und zu überwachen, sind Lieferketten aufgrund des komplexen Zusammenspiels verschiedener Elemente wie Unternehmen, Systemen, Informationen, Ressourcen, Menschen und Aktivitäten verwundbar. Darüber hinaus können veraltete Technologien, die z.T. über lange Zeiträume in der Produktion verwendet werden und keine Softwareservices mehr erhalten, leichter kompromittiert und Malware auf die damit verbundenen Systeme gespielt werden. Einzelne Branchen regeln die IT-Sicherheitsanforderungen sowie die damit verbundene Infor-

[20] Vgl. BSI 2017a, 4.
[21] Vgl. BSI 2019a, 11.
[22] 2017 wurden KMU mit 1 bis 499 Beschäftigten und große Unternehmen ab 500 berücksichtig. 2018 KMU mit 1 bis 249 Beschäftigten und große Unternehmen ab 250.
[23] Vgl. BSI 2019a, 7, 8.
[24] Vgl. BSI 2019b, 7.
[25] Vgl. McAfee 2018, 2.
[26] Vgl. ebd.
[27] Vgl. Symantec 2019a, 18.

mationssicherheit mit eigenen Branchen-Standards und Zertifizierungen (z.B. das Trusted Information Security Assessment Exchange - TISAX in der Automobilindustrie).[28] So kann die Sicherheit zwar einerseits branchenspezifisch erhöht werden, andererseits stellt die Erfüllung von unterschiedlichen Branchenstandards mithilfe eines Zertifizierungssystems eine weitere Herausforderung für KMU als Lieferanten und Dienstleister in der jeweiligen Branche dar.

Laut eines internationalen Reports von *CrowdStrike* aus dem vergangenen Jahr, an dem auch 200 (von ca. 1.300) deutsche IT-EntscheidungsträgerInnen und IT-SicherheitsexpertInnen teilgenommen haben, waren in etwa zwei Drittel der Unternehmen von mindestens einem Cyberangriff auf ihre **Lieferketten** betroffen.[29] Demgegenüber sieht nur etwa ein Drittel der Befragten die Sicherheit von Lieferketten als eine der Top-Prioritäten ihres Unternehmens und fast 80% sind der Meinung, dass ihr Unternehmen mehr für die Sicherheit der Lieferketten ausgeben sollte.[30]

Je kleiner das Unternehmen, desto geringer ist auch das Budget für IT-Sicherheit. Im Durchschnitt gaben Unternehmen in 2017 ca. 2.600 Euro für IT-Sicherheit aus, wobei die Investitionen mit der Unternehmensgröße stiegen.[31] 55% der Unternehmen mit 50 bis 249 MitarbeiterInnen verfügen über kein eigenes Budget für IT-Sicherheit.[32] In kleineren Unternehmen muss das Bewusstsein für Cybersicherheit bei Entscheidungsträgern vorhanden sein, damit geeignete technische und organisatorische Maßnahmen ergriffen werden können und das entsprechende Budget zur Verfügung steht. Fehlt diese Unterstützung von der **Geschäftsführung** bleiben Entscheidungen und Investitionen häufig aus. Dabei kann die Höhe der Investitionen beträchtlich variieren.[33]

Eine ganz grundsätzliche Organisationsentscheidung ist die Frage, wer im Unternehmen die **Verantwortung** für das Thema Cybersicherheit trägt und wer die Schutzmaßnahmen durchführt. Letzteres kann durch unternehmenseigenes Personal (*make*), oder durch externe Dienstleister (*buy*) erfolgen. Die Rolle der IT-Dienstleister bei der Herstellung von Schutzmaßnahmen für KMU ist bislang kaum untersucht und soll im Folgenden näher betrachtet werden.

5.3. Die Beschaffenheit des Deutschen IT-Sicherheitsmarktes (Anbieter)

5.3.1. Definition der IT-Dienstleister

Die IT-Branche ist kein traditionell gewachsener Wirtschaftsbereich, sondern aus verschiedenen Segmenten wie z.B. der Datenverarbeitung, Hardwareproduktion, Softwareentwicklung sowie IT-Services entstanden. Dadurch sind Abgrenzungskriterien nicht einheitlich definiert und unterscheiden sich je nachdem welche Quellen (Statistiken, Veröf-

[28] Vgl. DQS 2019, 6.
[29] Vgl. Crowd Strike 2018, 32.
[30] Vgl. ebd. 18, 19.
[31] Vgl. Wik 2017, 57.
[32] Vgl. TÜV 2019, 31.
[33] Vgl. KfW 2019, 7; Wik 2017, 57.

fentlichungen, Marktforschungsinstitute) bemüht werden. Die Branche ist einem ständigen Wandel in neue Geschäftsfelder ausgesetzt, was eine fortlaufende definitorische Abgrenzung und Anpassung nach sich zieht. Die in der amtlichen Statistik gebräuchlichen Klassifikation der Wirtschaftszweige (WZ) ermöglicht zwar eine Zuordnung spiegelt aber aus Sicht der Studie die agilen Marktentwicklungen und sich ändernden IT-Services nicht ausreichend wider.

IT-Dienstleister sind, nach derzeit gültiger Definition des *Statistischen Bundesamts*, Unternehmen, die **Dienstleistungen im Bereich der Informationstechnologien** erbringen.[34] Konkret beinhaltet dies „z. B. Anpassung, Testen und Pflege von Software, Planung und Entwurf von Computersystemen, die Hardware-, Software- und Kommunikationstechnologie umfassen, Verwaltung und Betrieb der Computersysteme und Datenverarbeitungsanlagen eines Kunden vor Ort sowie sonstige fachliche und technische mit der Datenverarbeitung verbundene Tätigkeiten."[35]

In der Klassifikation der Wirtschaftszweige werden im Wirtschaftsbereich der Hardware-Produktion (WZ 26) die Wirtschaftszweige Halbleiter (WZ 26.1), Datenverarbeitungsgeräte (WZ 26.2), Telekommunikationstechnik (WZ 26.3), Unterhaltungselektronik (WZ 26.4) und Herstellung von Datenträgern (WZ 26.8) aufgeführt.[36] Zudem die Wirtschaftsbereiche Telekommunikation (WZ 61), Erbringung von Dienstleistungen der Informationstechnologie (WZ 62), Informationsdienstleistungen (WZ 63) sowie der Wirtschaftszweig Reparatur von Datenverarbeitungs- und Telekommunikationsgeräten (WZ 95.1).[37]

IT-Dienstleistungen werden häufig auch als IT-Services beschrieben. IT-Dienstleistungen werden – unter Berücksichtigung des Untersuchungskontextes dieser Studie – für KMU erbracht, um deren Geschäftsprozesse und Wirtschaftlichkeit mit dem Einsatz von Informationstechnologie zu unterstützen, zu entwickeln, zu managen und weiter zu optimieren. IT-Dienstleistungen werden durch eine Kombination von Personen, Prozessen und Technologien erbracht.

Das Marktforschungsunternehmen *Lünendonk* widmet sich seit Jahren der Untersuchung von IT-Dienstleistungen und -Services und teilt diese in die nachfolgend erläuterten zwei Segmente ein.

Abzugrenzen von den IT-Dienstleistern sind demnach Unternehmen, die **Informationsdienstleistungen** im engeren Sinne erbringen, wie z.B. Datenverarbeitung und andere Tätigkeiten zur Erstellung von Informationen.[38] Zu berücksichtigen ist, dass IT-Sicherheit in der Statistik nicht explizit erfasst und ausgewiesen wird und somit in die Gesamtbetrachtung mit einfließt. Die *Lünendonk*-Studie 2019 unterscheidet hingegen zwischen IT-Beratungs- und Systemintegrationsunternehmen einerseits, die mehr als 60% ihres Umsatzes mit *Change-the-Business*-Leistungen (IT-Beratung,

[34] Vgl. Destatis 2019, 7.
[35] Ebd.
[36] Vgl. Destatis 2008, 18 ff.
[37] Ebd., 41 ff., 55.
[38] Vgl. Destatis 2019, 7.

Entwicklung von Individualsoftware, etc.) erwirtschaften, und IT-Service/-Dienstleistern andererseits, deren Tätigkeiten sich hauptsächlich um Wartungs-, Pflege-, Schulungs- und Unterstützungsleistungen (*support*) sowie um den Betrieb der Anwendungsumgebungen, Rechenzentren, Outsourcing, Infrastruktur- und IT-Plattformservices drehen.[39]

5.3.2. Marktgröße

Laut *Statistischem Bundesamt* betrug der Gesamtumsatz der Dienstleistungen in 2017 im Bereich der Informationstechnologien 134,4 Mrd. Euro – also etwas mehr als 4% des nominalen Bruttoinlandsprodukts.[40] Die Zahlen zum **Marktvolumen** der *Bitkom* weisen auf eine ähnliche Größenordnung hin und belaufen sich für das Jahr 2017 auf etwa 163 Mrd. Euro; wobei darunter sowohl die Informationstechnik mit 87,2 Mrd. Euro (IT-Hardware 25,2 Mrd. Euro, Software 23 Mrd. Euro und IT-Services 39 Mrd. Euro), als auch die Telekommunikation mit 65,5 Mrd. Euro (TK-Endgeräte 10,2 Mrd. Euro, TK-Infrastruktur 6,9 Mrd. Euro und Telekommunikationsdienste 48,5 Mrd. Euro) sowie die Unterhaltungselektronik (*Consumer Electronics*) mit 10 Mrd. Euro fallen, zu sehen in der folgenden Tabelle 5.[41]

Tabelle 5 Marktvolumen des Informations- & Telekommunikationsmarktes in Deutschland in 2017, Quelle: Bitkom & EITO 2019.

Informationstechnik	**87,2 Mrd. Euro**
IT-Hardware	25,2
IT-Services	39
Software	23
Telekommunikation	**65,5 Mrd. Euro**
TK-Endgeräte	10,2
TK-Infrastruktur	6,9
Telekommunikationsdienste	48,5
Consumer Electronics	**10 Mrd. Euro**
Gesamt	***162,7 Mrd. Euro***

Das Marktvolumen der IT-Dienstleistungen weist in den letzten drei Jahren ein kontinuierliches Wachstum von 2,3% auf.[42] Die *Lünendonk* Studie hat diese Zahlen aufgegriffen und darauf basierend errechnet, dass im Jahr 2018 ein **Marktanteil** von 63% auf die in der Studie analysierten 73 IT-Dienstleistungsunternehmen entfällt.[43] Damit repräsentieren die untersuchten 73 IT-Dienstleistungsunternehmen der *Lünendonk* Studie fast zwei Drittel des gesamten IT-Dienstleistungs-Marktes. Da eine trennscharfe Abgrenzung zu Dienstleistungen der IT-Sicherheit in der Erhebung nicht gegeben ist, werden sie zusammengefasst dargestellt und beziehen sich somit auf den IT-Dienstleistungsmarkt nach Definition von *Lünendonk*. Dies verdeutlicht, dass dieser grundsätzlich fragmentierte und diversifizierte Markt dennoch von einem hohen **Konzentrationsgrad** geprägt ist.

[39] Vgl. Lünendonk 2019, 5.
[40] Vgl. Destatis 2019, 7; siehe auch: www.destatis.de/Europa/DE/Thema/Basistabelle/Wirtschaft-Finanzen.html, Zugriff v. 14.02.2020.
[41] Vgl. Bitkom & EITO 2019, 1.
[42] Ebd.
[43] Vgl. Lünendonk 2019, 10.

5.3.3. Unternehmensgröße

Laut Ergebnisanalyse der Strukturerhebung im Dienstleistungsbereich durch das *Statistische Bundesamt,* sind in etwa 94.700 Unternehmen aus diesem Segment der Informationstechnologie zuzuordnen und etwa 13.300 Unternehmen als Informationsdienstleister erfasst.[44] Ein Großteil der Umsätze wird dabei von einigen wenigen Unternehmen generiert, wobei die 25 führenden IT-Beratungs- und Systemintegrationsunternehmen ca. 14,1 Mrd. Euro und somit mehr als ein Drittel des Marktvolumens erwirtschaften.[45]

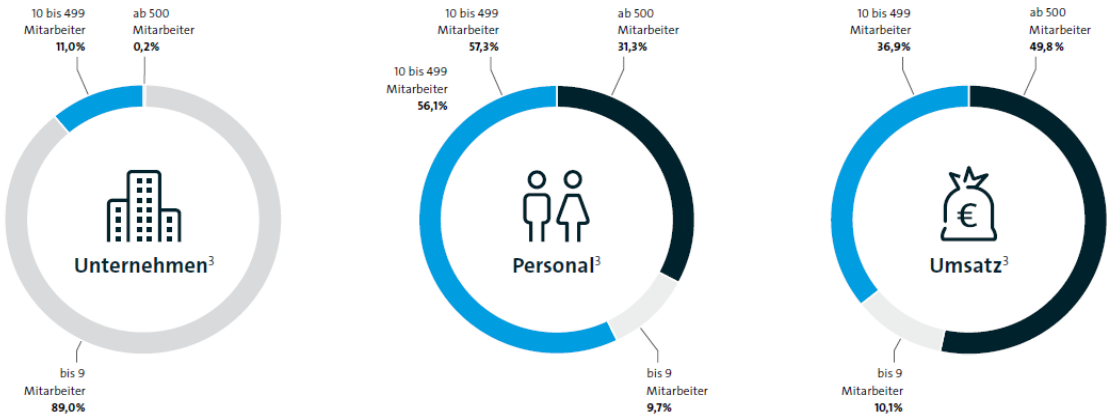

Abbildung 2 – Anzahl, Beschäftigte & Umsatz mittelständischer IT-Unternehmen, Quelle: Bitkom 2020a, 7.

Abbildung 2 **veranschaulicht** die **Unternehmensgrößenstruktur**, das Verhältnis von **Beschäftigtenzahlen**, sowie die **Umsatzverteilung** von IT-Unternehmen. Dabei wird die Bedeutung mittelständischer IT-Unternehmen für die Branche deutlich. 57% der sozialversicherungspflichtigen Beschäftigten arbeiten in 11% der Unternehmen und erwirtschaften 37% des gesamten Umsatzes in der Branche.

[44] Vgl. Destatis 2019, 4.
[45] Vgl. Lünendonk 2019, 11; & Bitkom & EITO 2019, 1.

5.3.4. Wachstum

Die **Umsatzentwicklung** im IT-Dienstleistungsbereich verläuft in den letzten Jahren überwiegend positiv. Die Branche konnte von ihrer Stellung als Wegbereiter der Digitalisierung profitieren. Abbildung 3 zeigt, zwecks eines Vergleichs, Veränderungen des realen Bruttoinlandprodukts (BIP) zu den Indizes des Umsatzes im Dienstleistungsbereich der Informationstechnologie. Sie verdeutlicht den überwiegend positiven Trend in der Branche, der selbst in Zeiten schwieriger Konjunkturphasen relativ konstant geblieben ist.

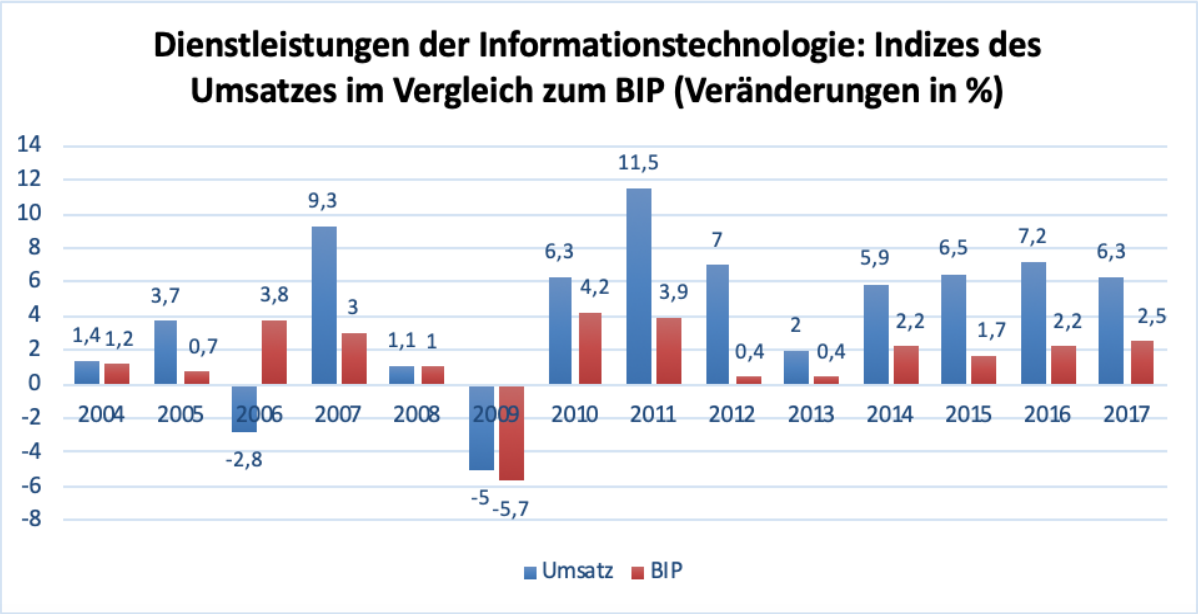

Abbildung 3 – Dienstleistungen der Informationstechnologie: Indizes des Umsatzes (Veränderungen in %),

Quelle: Eigene Darstellung basierend auf Berechnungen des Statistischen Bundesamtes.

Abbildung 4 zeigt die Umsatzindizes der Dienstleister in der Informationstechnologie. Zu sehen ist, dass diese sowohl die Indizes des übergeordneten IKT-Sektors als auch die anderer Dienstleistungssektoren in den letzten Jahren kontinuierlich übertroffen haben.

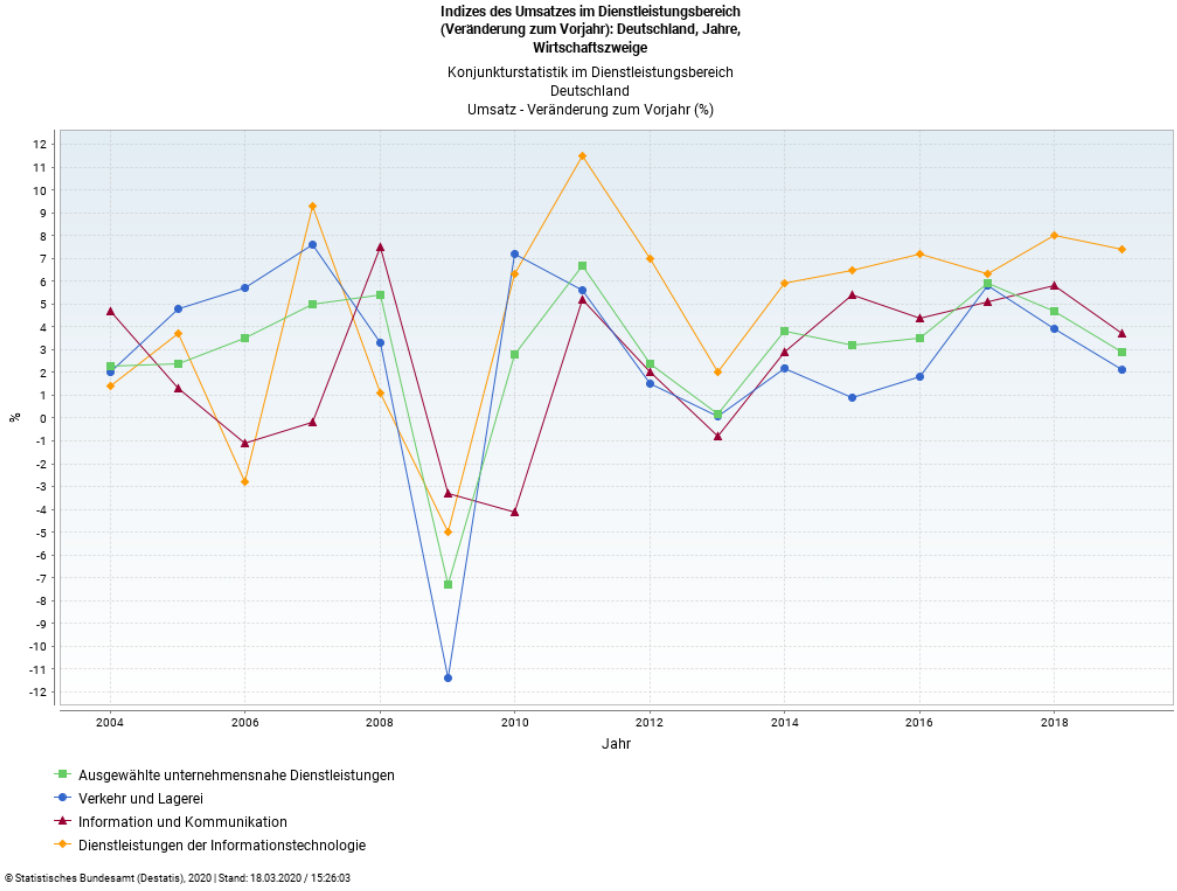

Abbildung 4 – Umsatzentwicklung im Dienstleistungsbereich, verschiedene Branchen,

Quelle: Eigene Darstellung basierend auf Berechnungen des Statistischen Bundesamt 2020.

Beginnend im Jahr 2011 hat das BIGS die Sicherheitswirtschaft mithilfe einer jährlichen Befragung analysiert. Dabei wurde die Sicherheitswirtschaft unterteilt in:

- Anbieter von Sicherheitstechnik,
- Anbieter von Sicherheitsdienstleistungen,
- (und ab 2017) Anbieter von IT-Sicherheit.

Im Zeitablauf zeigte sich allerdings, dass die Grenzen zwischen diesen Gruppen innerhalb der Sicherheitswirtschaft immer weiter verschwimmen. Dies liegt zum einen am allgemeinen Trend der Digitalisierung und zum anderen am wachsenden Kundenwunsch, Sicherheitslösungen aus einer Hand nachzufragen.[46]

[46] Rieckmann & Stuchtey 2018, 44 ff.

Abbildung 5 zeigt das erfasste Umsatzwachstum der vergangenen Jahre. Verglichen werden Bereiche der Sicherheitswirtschaft, die einen direkten Bezug zu Informationstechnologie, Digitalisierung und Elektronik haben, sowie Sektoren der klassischen Sicherheitsdienstleistungen (wie beispielsweise Wachschutz) in Relation zu der Gesamtwirtschaft in Deutschland. Letztere wird anhand des realen Bruttoinlandsprodukts abgebildet.[47] Wie aus der abgebildeten Zeitreihe ersichtlich ist, wächst der Umsatz der Sicherheitswirtschaft mit Bezug zu IT und Digitalisierung inklusive elektronischer Nicht-IT-Sicherheitsprodukten seit Jahren deutlich stärker als das reale Bruttoinlandsprodukt. Auch das Wachstum des nominalen Bruttoinlandsprodukts, das in den letzten fünf Jahren vor 2019 im Band zwischen 3 und 4% rangierte – hier nicht abgebildet – wird deutlich übertroffen.

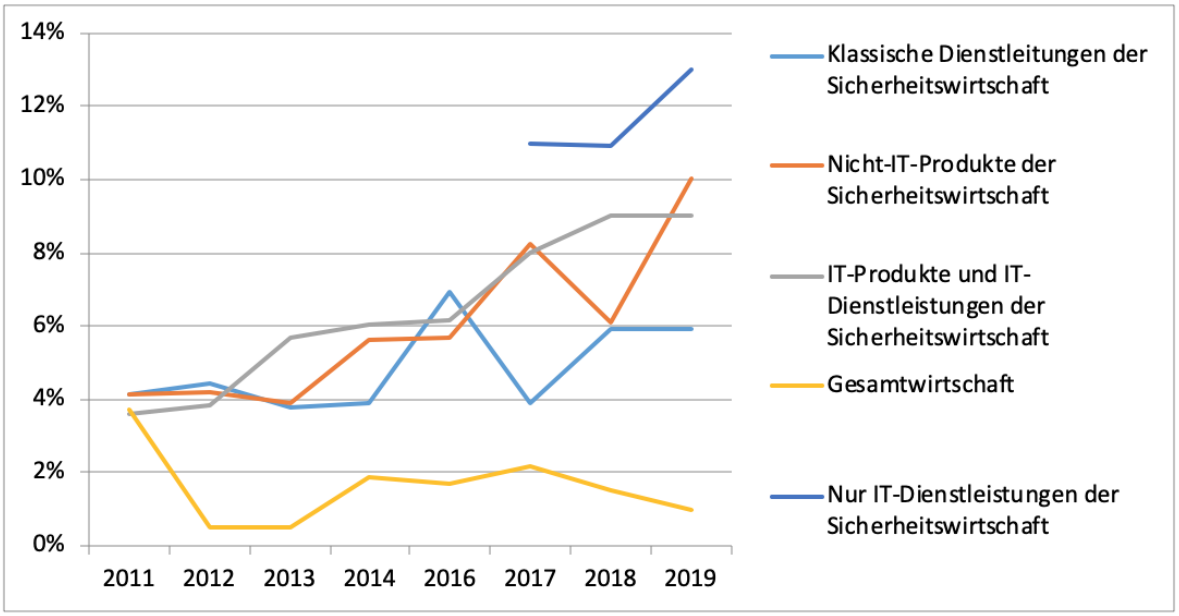

Abbildung 5 – Angaben zu Wachstumsentwicklung und -erwartung bis 2019, nach Angebotsportfolio, im Vergleich zur Gesamtwirtschaft. Quelle: Eigene Darstellung.

Die Sicherheitswirtschaft wächst ab dem Jahr 2011 in allen **Bereichen deutlich überdurchschnittlich**. Das steile Umsatzwachstum der klassischen Sicherheitsdienstleistungen ab 2015 muss rückblickend als Sondereffekt betrachtet werden, der maßgeblich auf die Flüchtlingskrise zurückzuführen ist. Heute sind es vor allem die Bereiche der elektronischen Sicherheitstechnik sowie der IT-Produkte und IT-Dienstleistungen, die das stärkste Umsatzwachstum vermelden. Da für den Bereich der IT-Dienstleistungen der Sicherheitswirtschaft keine separaten Angaben verfügbar sind, können in der vorliegenden Zeitreihe jedoch nur Daten ab 2017 dargestellt werden.

[47] Fortgeschriebene Abbildung auf Basis von Stuchtey, Rieckmann (2018): Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung, in: Kompendium Sicherheit – Gesellschaft – Digitalisierung von Günter Calaminus (Hrsg.), TCC Verlagsgesellschaft, 2018, S. 56 (Abbildung 2). Zugrundeliegende Datenquellen: BIGS (2011-2017), Bitkom (2018c), Heuer (2018), ISG Information Services Group (2018), Security Essen (2018), Statista (2018), BMWi (2019). Daten für die Kurve „Nur IT-Dienstleistungen der Sicherheitswirtschaft“ liegen nicht für die gesamte Zeitreihe vor.

Gleichzeitig sind laut *Lünendonk* einige IT-Dienstleister, aufgrund der angespannten Situation auf dem Arbeitsmarkt für IT-Fachkräfte und dem großen Bedarf Projekte annehmen und durchführen zu können, vorsichtiger mit ihren Umsatzprognosen und erwarten ein langsameres Wachstum.[48] Darüber hinaus wirken sich die Konjunktursorgen der Weltwirtschaft in Branchen wie z.B. der Chemie- und Automobilindustrie sowie dem verarbeitenden Gewerbe teilweise auf Investitionen in Digitalisierungsprojekte aus, was ebenfalls zu vorsichtigeren Wachstumsprognosen einiger IT-Dienstleister führt.[49] Beratungstätigkeiten bedürfen branchenspezifischer Kenntnisse zu Geschäftstätigkeiten und Prozessen, weshalb IT-Dienstleister üblicherweise nicht alle Branchen bedienen können. Die Spezialisierung führt jedoch dazu, dass rückläufige Umsätze in einzelnen Branchen nicht einfach durch andere aufgefangen werden können.[50] Trotz der Eintrübung der Weltwirtschaft und den damit verbundenen Auswirkungen für Deutschland sind die Auftragsbücher der in der *Lünendonk* Studie untersuchten IT-Dienstleister gut gefüllt, weshalb sich die Hauptsorge auf den Mangel an Fachkräften fokussiert.[51]

5.3.5. Entwicklung des Produktportfolios

Die *it-sa Benefiz e.V.* hat 2014 eine Umfrage durchgeführt, an der insgesamt 82 IT-Dienstleister aus dem süddeutschen Raum teilgenommen haben. Die Ergebnisse dieser Umfrage veranschaulichen, dass kleine und mittlere IT-Dienstleister im Geschäftskundenstamm vor allem Klein- und Kleinstunternehmen betreuen, die ihrerseits weniger als 50 MitarbeiterInnen beschäftigen.[52]

IT-Sicherheitslösungen machen bei zwei Dritteln der Befragten nur einen geringen Anteil am Umsatz aus.[53] Das Produktportfolio reicht dabei von Basisleistungen bis hin zu fortgeschrittenen IT-Schutzmaßnahmen. Solche fortgeschrittenen Maßnahmen, wie z.B. der Aufbau eines Managementsystems für Informationssicherheit, IT-Forensik oder Penetrationstests, werden von kleinen IT-Dienstleistern nur selten angeboten.[54] Der Angebotsrahmen befasst sich vorwiegend mit Basisleistungen der ersten Generation wie beispielsweise Virenschutz und einer Firewall.

Durch die Zunahme softwarebasierter Produkte und Dienstleistungen, sowie der Digitalisierung von analogen und manuellen Prozessen (digitale Transformation) sind Unternehmen häufig auf externe Beratungsleistungen angewiesen.[55] Zu den am meisten gefragten IT-Dienstleistungen im Jahr 2018 gehören laut der *Lünendonk* Studie die Integration digitaler Lösungen in die Backend-IT mit 85%, die agile Anwendungsentwicklung mit 76%, Big Data Analytics mit 74%, Kundenerfahrung und digitale Kundenschnittstellen mit 73%, Hybride Cloud/Orchestrierung mit 68% sowie IT-

[48] Vgl. Lünendonk 2019, 12.
[49] Ebd.
[50] Ebd.
[51] Ebd., 15.
[52] Vgl. it-sa 2014, 2.
[53] Vgl. it-sa 2014, 3.
[54] Vgl. it-sa 2014, 2.
[55] Vgl. Lünendonk 2019, 22.

und Datensicherheit mit 67%.[56] In allen genannten IT-Dienstleistungsbereichen wächst die prognostizierte Nachfrage für die Jahre 2019 und 2020 zwischen 2 und 14%.[57]

Neben der Systemintegration, dessen Aufgabe es ist neu entwickelte Softwarelösungen in die bestehende IT-Landschaft (*Backend-IT*) zu integrieren, spielen *Frontend*-Lösungen in Form von Applikationen, die mit bestehenden IT-Systemen und der Prozesslandschaft vernetzt werden, sowie die Vernetzung/Orchestrierung verschiedener Cloud-Lösungen eine wichtige Rolle in der Entwicklung des Produktportfolios von IT-Dienstleistern. Durch die verbesserten Sicherheitsstandards und Anwendungsmöglichkeiten von Cloud-Systemen wird erwartet, dass viele Unternehmen ihre Datenbanken in die *digitale Wolke* verlagern.[58] Durch die Zunahme der gesammelten Daten in Bereichen wie dem Internet der Dinge (IoT – *Internet of Things*), der Industrie 4.0, oder dem *E-Commerce*, benötigen Unternehmen Unterstützung bei der Datenanalyse.

Knapp 59% der erzielten Umsätze im Jahr 2018 entfallen auf den Industrie- sowie den Finanzdienstleistungssektor und machen diese Sektoren zu den wichtigsten Kundenbranchen für die in der *Lünendonk* Studie untersuchten IT-Dienstleister.[59] Während die Automobilbranche mit einem Anteil von rund 16%, die umsatzstärkste Einzelbranche innerhalb des Industriesektors (ca. 34%) ausmacht und als Wachstumstreiber fungiert, ist die Bankenbranche mit rund 17% das Zugpferd des Finanzdienstleistungssektors.[60]

Nicht nur die Umsatzentwicklungen der letzten Jahre, sondern auch die Fusions- und Übernahme- (*Mergers and Acquisitions*) Aktivitäten bei einigen IT-Dienstleistern zeigen, dass der IT-Markt in Bewegung ist.[61] Der Prozess der Konsolidierung hat zum einen das Ziel, einzelne Funktionsbereiche zu verstärken und sich spezifisches Know-how zuzukaufen,[62] und zum anderen ist er im steigenden Margendruck und dem stetig wachsenden Investitionsbedarf aufgrund immer kürzer werdender Innovationszyklen begründet.[63] Vor diesem Hintergrund ist ebenfalls zu beobachten, dass strategische Partnerschaften und Joint Venture eingegangen werden, um dem Fachkräftemangel zu begegnen, spezielle Kompetenzen und Dienstleistungen zu teilen und den wirtschaftlichen Druck besser abzufedern.[64]

[56] Ebd.
[57] Ebd.
[58] Ebd., 24.
[59] Ebd., 26.
[60] Ebd.
[61] Ebd., 52.
[62] Ebd.
[63] Vgl. IT-Onlinemagazin 2019.
[64] Vgl. Lünendonk 2019, 28; Systemhaus 2018, 28; IT-Onlinemagazin 2019.

5.3.6. Sonstiges: Kundenakquisition, Regionalität, Humankapital

Die **Kundenakquisition** beruht oftmals auf persönlichen Kontakten und erfolgt auf (mündliche) Empfehlung.[65] Hat ein KMU einen Dienstleister einmal engagiert, so werden häufig im Nachgang alle IT-Lösungen von diesem Anbieter bezogen, auch wenn **ggf. ein Wettbewerbsvorteil des Dienstleisters nicht in allen Bereichen vorhanden ist.**[66]

Die in der *Lünendonk* Studie untersuchten IT-Dienstleister haben neben dem Bestandskundengeschäft den Neukundenbereich im Jahr 2018 weiter ausgebaut. Mehr als 20% des Gesamtumsatzes wurde bei 31% der IT-Dienstleister durch **Neukunden** generiert.[67]

Die *Systemhausstudie* merkt darüber hinaus an, dass Regionalität und räumliche Nähe ein wichtiger Faktor bei der Kundengewinnung sind.[68] Bei der Betrachtung der Verteilung der Unternehmen im Wirtschaftszweig der Erbringung von Dienstleistungen der Informationstechnologie, werden regionale Cluster nach Bundesländern deutlich. Dabei stechen Bayern, Nordrhein-Westfalen, Baden-Württemberg, Hessen und Berlin besonders hervor. Darüber hinaus zeigt sich, dass auch in Niedersachsen, Hamburg und Rheinland-Pfalz eine Vielzahl von Unternehmen im Bereich der Dienstleistungen der Informationstechnologien angesiedelt sind.

Dieses Bild deckt sich mit anderen Lagebildern über die Verteilung der IT-Dienstleister in Deutschland. Die Deutschlandkarte der besten IT-Dienstleister des Wirtschaftsmagazins *brand eins* beispielsweise listet 204 Unternehmen auf, die gehäuft in Berlin, München, Hamburg, Stuttgart, Köln (einschließlich des Rheinlands und des Ruhrgebiets) sowie Frankfurt am Main und Nürnberg vorzufinden sind.[69] Wenngleich oftmals nur größere IT-Dienstleister (nach Umsatz, Zahl der MitarbeiterInnen und Niederlassungen) bei solchen Erfassungen berücksichtigt werden, deckt sich diese geographische Verteilung mit Erkenntnissen anderer Netzwerke die dieser Branche nahestehen.[70]

Die neuen Bundesländer scheinen, was die Wahl des Standortes betrifft, deutlich weniger attraktiv für IT-Dienstleister zu sein – abgesehen von einigen wenigen größeren Unternehmensansiedlungen in Städten wie Leipzig oder Dresden. Abbildung 6 macht diesen Unterschied zwischen den neuen und alten Bundesländern deutlich.

[65] Vgl. it-sa 2014, 2.
[66] Vgl. Wik 2017, 33.
[67] Vgl. Lünendonk 2019, 11.
[68] Vgl. Systemhaus 2018, 28.
[69] Siehe https://www.brandeins.de/magazine/brand-eins-thema/it-dienstleister-2020/interaktive-karte-und-bestenliste
[70] Siehe ITeams, ComTeam, BitMe.

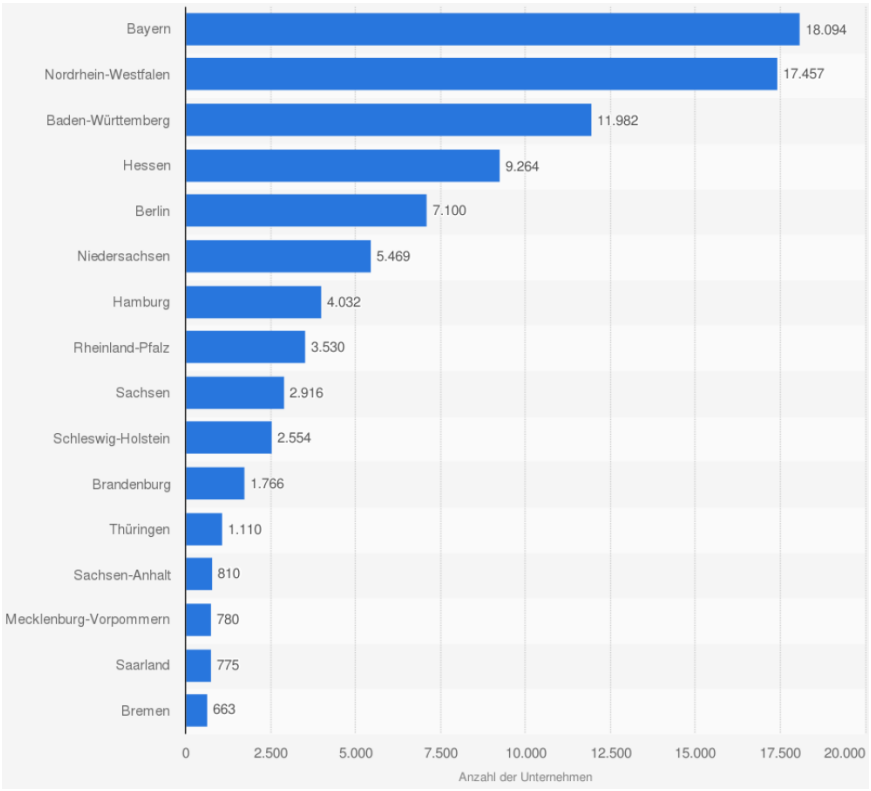

Abbildung 6 – Anzahl der steuerpflichtigen Unternehmen* des Wirtschaftszweiges "Erbringung von Dienstleistungen der Informationstechnologie (WZ 62)" in Deutschland im Jahr 2018 nach Bundesländern.

Quelle: Statistisches Bundesamt, Statista 2020.

Aus Sicht der IT-Dienstleister spielen Qualifikation, Zertifizierung und Kosten des Dienstleisters eine geringere Rolle als das vertrauensvolle persönliche Verhältnis.[71] Deutlich mehr als die Hälfte der befragten IT-Dienstleister ist der Ansicht, dass die fachliche Ausbildung, nachgewiesene Weiterbildung der MitarbeiterInnen oder Zertifizierungen des Dienstleistungsbetriebs nicht allzu relevant sind.[72]

Aus der *it-sa* Umfrage geht hervor, dass die Gestaltung der Zusammenarbeit lediglich bei der Hälfte der befragten IT-Dienstleister vertraglich vereinbart wird und dass von Seiten der IT-Dienstleister **Sicherheitslösungen** wenig bis gar **nicht beworben** werden (immerhin 26% bewerben gar nicht) und die Angebote von Uneinheitlichkeit geprägt sind.[73] Marketing und Vertragsgestaltung sind durch einen vergleichsweise niedrigen Grad an Formalisierung gekennzeichnet.

[71] Vgl. it-sa 2014, 16.
[72] Ebd., 15.
[73] Vgl. it-sa 2014, 14, 3.

Einschränkend muss angemerkt werden, dass die *it-sa* Studie einen regionalen Fokus aufweist und dass ihre Aussagekraft aufgrund ihres Entstehungsjahres und der Dynamik der Thematik etwas limitiert ist. Gleichwohl wird es interessant sein, ob die Aussagen in der folgenden Befragung von ihrer Tendenz repliziert werden können.

Ein laufendes Problem (auch) für die IT-Dienstleister ist der Mangel an qualifiziertem **Humankapital**. So können Projekte teilweise nur deshalb nicht umgesetzt werden, weil IT-ExpertInnen fehlen.[74] Laut *Bitkom* erreichte die Zahl der offenen Stellen für IT-ExpertInnen ein Rekordhoch von 124.000 in 2019 und lag damit 51% höher als im Vorjahr.[75] Die Top 20 mittelständischen IT-Beratungen, die nach Definition von *Lünendonk* ihren Hauptsitz in Deutschland haben und einen Umsatz von bis zu 500 Mio. Euro aufweisen, konnten nahezu jede zehnte Stelle aufgrund des **Fachkräftemangels** nicht besetzen und mussten in etwa jede fünfte Projektanfrage ablehnen.[76] In Anbetracht der steigenden Bedeutung der IT- und Cybersicherheitsbranche und dem damit einhergehenden Wachstum der Nachfrage nach Fachkräften, stellt dieser Mangel ein ernstzunehmendes Wachstumshemmnis dar. Darüber hinaus trägt die Qualifikation der MitarbeiterInnen zur Qualität der Dienstleistungen bei. Unternehmen, die sich mit Cybersicherheit beschäftigen, stehen in einem ständigen Wettbewerb mit Cyberkriminellen. Dementsprechend sind konsequente Weiterbildungsmaßnahmen notwendig, um der dynamischen Entwicklung in diesem Umfeld und dem digitalen Wechselspiel zwischen Offensive und Defensive Rechnung tragen zu können. Dies führt u.a. dazu, dass IT-Dienstleister ihre MitarbeiterInnen im Verbund mit Hoch- und Fachhochschulen selbst ausbilden und Personalmarketing aktiver betrieben wird.[77]

Angesichts der Verantwortung, die IT-Dienstleister gegenüber ihren Kunden haben, sind auch Investitionen in die eigene Unternehmenssicherheit elementar für die eigene Geschäftsgrundlage. Wie das *BSI* im *Lagebericht 2019* berichtet, sind mittlerweile vermehrt **IT-Dienstleister selbst Opfer** von Cyberangriffen.[78]

5.4. KMU als Nachfrager von IT-Sicherheit

Kleine und mittlere Unternehmen stehen vor der Entscheidung, ob sie ihre IT-Sicherheit eigenen MitarbeiterInnen überlassen (*make*) oder hierauf spezialisierte Dienstleister am Markt einkaufen (*buy*). Wie in vielen Bereichen der Digitalisierung, ist auch die IT-Sicherheit mit erheblichen **Skaleneffekten** verbunden. Je kleiner ein Unternehmen ist, desto größer wird der Anteil, der auf die Absicherung der IT-Systeme und Daten aufgewendet werden muss. Je kleiner ein Unternehmen ist, desto wahrscheinlicher ist es daher auch, dass die *Make-or-Buy*-Entscheidung zu Gunsten eines

[74] Vgl. Lünendonk 2019, 12.
[75] Vgl. Bitkom 2020a, 27.
[76] Vgl. Lünendonk 2019, 18.
[77] Ebd.; siehe auch: Partnerfirmen der FH-Aachen www.fh-aachen.de/fachbereiche/medizintechnik-und-technomathematik/einrichtungen/sp-studienortkoeln/partnerfirmen/, Zugriff v. 14.02.2020.
[78] Vgl. BSI 2019b, 49.

externen Dienstleisters ausgeht. So haben insbesondere größere Unternehmen tendenziell eher eine eigene IT-Abteilung. Kleinere Unternehmen geben sowohl in absoluten als auch in relativen Zahlen weniger für ihre IT-Sicherheit aus.[79]

Aus dem Blickwinkel der IT-Sicherheit stellt sich damit die Frage, wie und nach welchen Kriterien die Entscheidung für einen konkreten IT-Dienstleister getroffen wird und welche expliziten Leistungen von diesem eingekauft werden. In diesem Abschnitt soll daher die Rolle von KMU als Nachfrager von IT-Sicherheitsdienstleistungen betrachtet werden.

Während noch im Jahr 2011 große Unternehmen mit mehr als 2.500 MitarbeiterInnen die Hälfte der dokumentierten Cyberangriffe verzeichneten (18% der KMU mit bis zu 250 MitarbeiterInnen), hat sich die Opferpyramide in den darauffolgenden Jahren umgekehrt.[80] 2016 verzeichneten laut dem *Symantec Threat Report* bereits 43% der KMU einen Cyberangriff, aber „nur" noch 35% der Großunternehmen.[81] Andere Studien sehen Großunternehmen unverändert im Fokus von Cyberkriminellen und verweisen auf steigende Fallzahlen über Unternehmensgrößen hinweg.[82] Teilweise verdeutlichen sie jedoch auch ein Verkennen der Bedrohungslage innerhalb kleinerer Unternehmen, da diese glauben, sie seien zu klein oder unwichtig, um ins Fadenkreuz von Cyberkriminellen zu geraten.[83]

Ein Erklärungsansatz hierfür sind die Strukturmerkmale in KMU, die, wie weiter oben erläutert, beim Thema Sicherheit zum einen mit der Unternehmensgröße und der Bereitschaft in der Unternehmensleitung zusammenhängen, Cybersicherheit nicht nur als Kostenfaktor, sondern als notwendige Bedingung für ein erfolgreiches Geschäftsmodell zu betrachten. Da dies häufig nicht der Fall ist, werden Investitionen aufgrund des Mangels an sichtbaren Erfolgsfaktoren in der Cybersicherheit gescheut. Darüber hinaus haben sich Großunternehmen in den vergangenen Jahren in Bezug auf ihre Cyberabwehr besser gerüstet und sind für „herkömmliche" Cyberkriminelle schwerer zu erreichen. Damit rücken die *Low-Hanging-Fruits*, die einfacheren aber vielleicht nicht ganz so offensichtlichen Opfer, in den Fokus der Cyberkriminellen. Die zunehmende Digitalisierung der KMU und die damit gestiegene Verwundbarkeit im Netz können ebenfalls als Erklärung für steigende Fallzahlen hinzugezogen werden.

Organisatorische sowie technische Vorkehrungen wie Forensik, Penetrationstests oder *Intrusion Detection* Systeme für eine erhöhte Sicherheit informationstechnischer Systeme sind in KMU häufig nicht vorhanden.[84] Managementsysteme für Informationssicherheit (Information Security Management System - ISMS), wie sie z.B. nach den Vorgaben von § 8a Abs. 1 des BSI-Gesetzes für Betreiber Kritischer Infrastrukturen gesetzlich verpflichtend sind,[85] fehlen oftmals in KMU.[86] Die letzte Cyber-Sicherheits-Umfrage des *BSI* im Betrachtungszeitraum 2018 ergab, dass nur etwa 37% der

[79] Vgl. Park et al. 2008, 92.
[80] Vgl. Symantec 2016, 43.
[81] Ebd.
[82] Vgl. Bitkom 2020b, 8; BSI 2019a, 11 ff.
[83] Vgl. GDV 2018, 8.
[84] Vgl. Bitkom 2020b, 34 ff.
[85] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG), § 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen.
[86] Vgl. BSI 2019b, 50.

KMU[87] einen ganzheitlichen Ansatz bei der Cybersicherheit verfolgen und ein ISMS betreiben, während es bei großen Unternehmen 61% sind.[88] Die Qualität der Cybersicherheit von KMU ist jedoch durch Umfragen schwer zu ermitteln, da zum einen davon ausgegangen werden kann, dass sich eher IT-affine Unternehmen an solchen Umfragen beteiligen, die sich bereits in IT-Sicherheits-Netzwerken befinden oder damit in Kontakt stehen und zum anderen der Begriff „KMU" weit gefasst ist. Darüber hinaus benötigen nicht alle KMU ein ISMS - abhängig von Größe und dem prozessorientierten Ansatz innerhalb des Betriebs - auch wenn es oftmals wünschenswert wäre. Da viele KMU ihre Unternehmensprozesse nicht kennen und somit ein umfassendes Verständnis fehlt, ist es vielfach nicht umsetzbar.

Eine Studie des IT-Sicherheitsunternehmens *Symantec* zeigt, dass Wissen in der Cybersicherheit schnell veraltet und IT-ExpertInnen in der Branche aufgrund des **Fachkräftemangels** überarbeitet sind. Demnach gaben 51% der befragten deutschen Cybersicherheits-Verantwortlichen aus dem mittleren und gehobenen Management an, dass ihr Team zu ausgelastet ist, um sich über neue Entwicklungen zu informieren, während 45% der Meinung waren, dass ihr Team nicht ausreichend qualifiziert ist, um Cyberbedrohungen adäquat entgegenzutreten.[89] Die Arbeitsbelastung und die damit verbundene fehlende Zeit für Weiterbildung führen laut der *Symantec* Studie dazu, dass etwa zwei Drittel der Befragten darüber nachdenken, ihren Job oder die Branche zu wechseln.[90] Somit stellt sich für Unternehmen nicht nur die Herausforderung, neue MitarbeiterInnen für das Unternehmen zu gewinnen, sondern auch die bestehenden Teammitglieder beisammen zu halten.

Sicherheit ist schwer zu messen und daher häufig eine gefühlte bzw. **subjektive Sicherheit,** statt einer objektiven, welche sich an konkreten Kennzahlen abmessen ließe. Diese Aussage gilt für Sicherheit im Allgemeinen, aber auch für die Cybersicherheit. Gerade in KMU ist man daher vom Sicherheitsgefühl der Geschäftsleitung abhängig, wenn es um die Zuteilung eines Budgets für IT-Sicherheit geht. Oftmals ändert sich das Sicherheitsgefühl erst durch den Eintritt eines Schadenfalls, wenn nur noch reaktiv gehandelt werden kann.

[87] N=1039 Unternehmen, davon 57% mit 1 bis 249 Beschäftigte (≈592,23 > 592 KMU).
[88] Vgl. BSI 2019b, 50; BSI 2019a, 18.
[89] Vgl. Symantec 2019b, 9.
[90] Ebd.

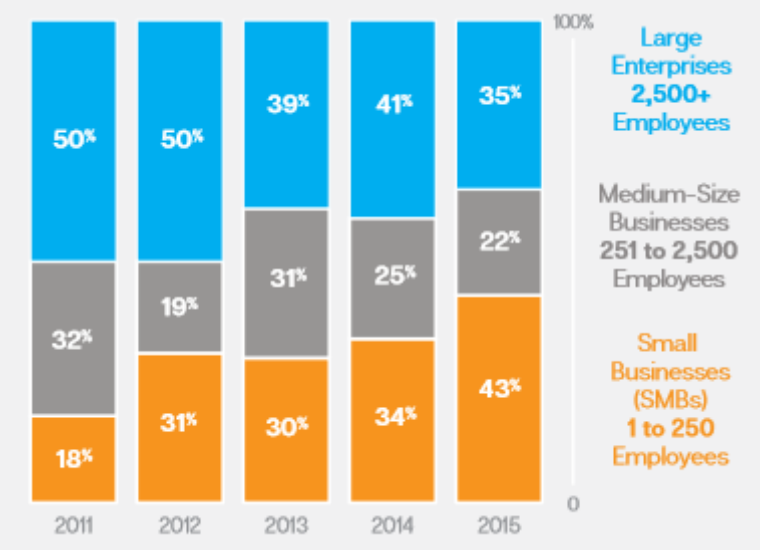

Abbildung 7 – Spear-Phishing-Angriffe nach Unternehmensgröße in %, Quelle: Symantec 2016, 43.

5.4.1. Informationsasymmetrie

Wertschöpfungsketten werden aufgrund der Digitalisierung neu zusammengesetzt und immer häufiger in der einen oder anderen Form mit dem Internet verbunden. Durch diese Verbindung erhöht sich das Risiko, Opfer eines Cyberangriffs zu werden, weil die Anzahl der Angriffspunkte zunimmt. Dieser Zusammenhang besteht unabhängig von der Unternehmensgröße. Die weltweiten Schäden, die durch Cyberkriminalität verursacht werden, sollen gem. *Cybersecurity Ventures* bis 2021 auf bis zu 6 Billionen US-Dollar ansteigen.[91]

Vergleichbare Zahlen gibt es viele und sie stammen in der Regel aus Studien von Cybersicherheitsunternehmen, die natürlich ein **Eigeninteresse** daran haben, die Bedrohung besonders hoch wirken zu lassen, um in der Folge dem verängstigten Unternehmer Hilfe verkaufen zu können. Dabei besteht in der Regel das Problem einer **asymmetrischen Informationsverteilung** in Bezug auf die Qualität des angebotenen Schutzgutes. Für ein Unternehmen, und ganz besonders für KMU, ist es schwierig bzw. kostspielig herauszufinden, von welcher Qualität ein bestimmtes Schutzgut für den Cyberraum ist. Unter anderem führen diese **Informationskosten** dazu, dass größere Unternehmen es leichter haben sich effektiver vor Cyberangriffen zu schützen, da sich für sie die höheren Kosten aufgrund von Größeneffekten besser auf einzelne Produkte verteilen lassen. Die Informationskosten sind weitgehend unabhängig von der Unternehmensgröße und erzeugen **Skaleneffekte** bei der Ausnutzung der Information. Für kleinere Unternehmen sind die

[91] Vgl. Cybersecurity Ventures 2020, 2.

Informationskosten also relativ höher als für große Unternehmen, sofern die Skaleneffekte letzterer nicht durch erhöhte Suchkosten überkompensiert werden. In der Folge sind kleinere Unternehmen tendenziell schlechter geschützt als große Unternehmen.[92]

Die von staatlichen Institutionen zur Verfügung gestellten **Lageberichte** sind bislang noch nicht hinreichend, um für KMU als Grundlage für die Allokation ihres Budgets für IT-Sicherheitsmaßnahmen zu dienen.[93] Risikoinformationen im Cyberraum werden noch nicht ausreichend gesammelt bzw. in verwertbarer Weise veröffentlicht, sodass adäquate Maßnahmen von Unternehmen nicht ergriffen werden können. Großunternehmen helfen sich durch freiwillige Zusammenschlüsse zum Austausch von Informationen über Bedrohungen und konkrete Angriffe auf Partner in diesen Zirkeln.[94] Dieser Aufwand ist für KMU in der Regel prohibitiv hoch.

Der Markt für IT-Sicherheitsprodukte und Dienstleistung unterliegt vielfach einer **adversen Selektion**, da die Kunden über wenig vertrauensvolle Informationen bzgl. der Qualität der Produkte verfügen.[95] Defizienter Transfer solcher Qualitätsinformationen zwischen den Marktseiten wird in den Wirtschaftswissenschaften spätestens seit Akerlofs "*Market for Lemons*" diskutiert.[96] Anderson hat diese Überlegung auf Märkte für IT-Sicherheitsprodukte übertragen.[97]

Die Komplexität der Materie und auch die dynamischen Entwicklungen zahlreicher Sicherheitstools erhöhen den Beratungsbedarf.[98] Das bestehende Angebot an Sicherheitsmaßnahmen überfordert viele, insbesondere aber kleine Unternehmen, die nicht einschätzen können, welche Angebote für sie von Relevanz sind.[99]

Aufgrund einer mit Blick auf die Produktqualität bestehenden Sichtblende können die Nachfrager zwar den Preis, nicht aber die Qualität erkennen (siehe dazu Abbildung 8). Daher fehlt es auch an einer Zahlungsbereitschaft für besonders hochwertige IT-Sicherheitsprodukte und Dienstleistungen, ohne die IT-Dienstleister keinen Anreiz haben, hochwertige Schutzleistungen anzubieten. Daraus resultierend können sich diese Leistungen am Markt nicht durchsetzen.[100]

[92] Vgl. Wik 2017, 77.
[93] Vgl. Bretschneider, W.; Rieckmann, J.; Stuchtey, T.; Szanto, A. 2020, 140.
[94] Vgl. Charter of Trust, z.B. https://www.charteroftrust.com/ Zugriff v. 14.02.2020.
[95] Vgl. Anderson 2001, 5-6.
[96] Vgl. Akerlof 1970; in der Literatur wird das unter dem Begriff der asymmetrischen Information (zu Lasten des Nachfragers), der verborgenen Eigenschaften (hidden characteristics) oder der adversen Auslese (adverse selection) diskutiert.
[97] Ebd., 7 ff.
[98] Vgl. Senseon 2019, 4.
[99] Vgl. Wik 2017, 44.
[100] Vgl. Moore 2010, 8.

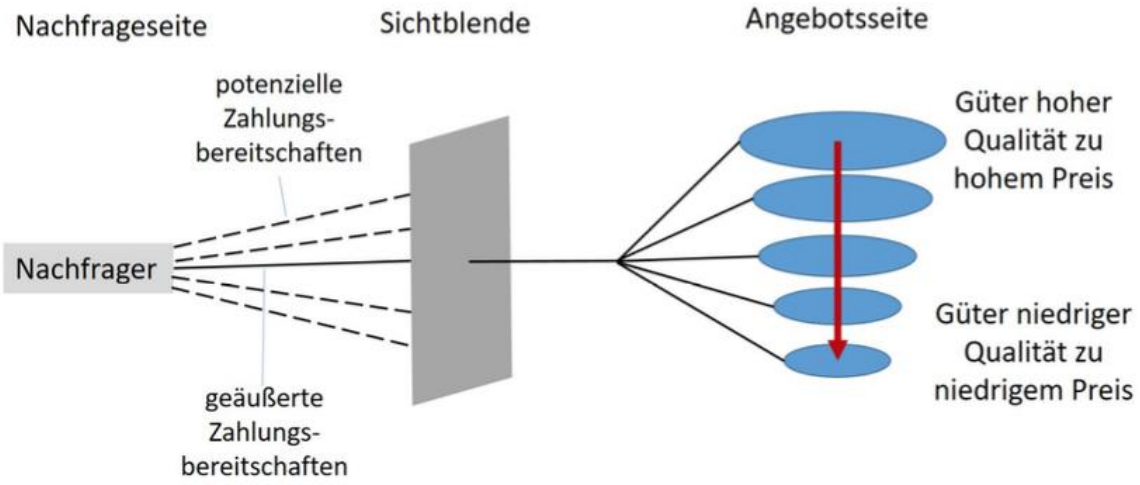

Abbildung 8 – Nachfrageverhalten mit asymmetrischer Informationsverteilung, Quelle: Fritsch 2018, 252.

Da im Cybersicherheitsbereich der Mensch oftmals das schwächste Glied in der Sicherheitskette darstellt,[101] sind KMU aufgrund fehlender bzw. nicht ausreichender **Schulungen der MitarbeiterInnen** hier besonders gefährdet.[102]

Bislang hat nur eine Minderheit der Unternehmen in Deutschland ausreichende organisatorische IT-Sicherheitsmaßnahmen eingeführt z.B. die Etablierung eines Managementsystems für Informationssicherheit,[103] regelmäßige Weiterbildung, Trainings und Übungen oder die Durchführung von regelmäßigen **Sicherheitsaudits** durch externe Berater.[104]

5.4.2. IT-Sicherheitsmaßnahmen

Gemäß dem BMWi geben 15% der deutschen Industrieunternehmen **Sicherheitsbedenken als Hemmnis der Digitalisierung** an.[105] Letztlich bedeutet dies, dass mögliche Produktivitätsfortschritte nicht wahrgenommen werden, weil es mit verhältnismäßigen Kosten nicht möglich ist, die hierdurch entstehenden Risiken hinreichend zu managen. Die wiederum dadurch entstehenden Wettbewerbsnachteile werden wissentlich in Kauf genommen, wobei es sich bei diesen Angaben um Unternehmen handelt, die eine bewusste Entscheidung treffen. Es ist davon auszugehen, dass viele Unternehmen ohne eine hinreichende Bedrohungsanalyse und Risikomanagement die Reise in die Digitalisierung antreten.

[101] Vgl. Accenture 2019, 6; Symantec 2019, 22.
[102] Vgl. BSI 2017a, 16; Wik 2017, 59.
[103] Vgl. BSI 2019b, 50.
[104] Vgl. Bitkom 2020b, 37ff.
[105] Vgl. BMWi, https://www.mittelstand-digital.de/MD/Redaktion/DE/Dossiers/A-Z/it-sicherheit.html, Zugriff v. 14.02.2020.

So wird laut *BSI* ein Cybersicherheits-Monitoring nur von einer Minderheit der KMU durchgeführt.[106] Zudem verzichteten nach einer Studie von *Deutschland sicher im Netz* (DsiN) auch beispielsweise im Jahr 2018 mehr als 40% der KMU auf eine regelmäßige Aktualisierung ihrer Software und Systeme (sog. Patches).[107] Diese Zahl hat sich auch im letzten Report von 2020 nur geringfügig verkleinert.[108] Wenig verwunderlich hingegen ist das Ergebnis der *Bitkom*, dass nur eine Minderheit der Unternehmen fortgeschrittene, technische Maßnahmen wie Penetrationstests und Intrusion Detection Systeme verwenden.[109] Schon früh wurde vom *BSI* auf die Umsetzungslücke in Bezug auf IT-Sicherheit,[110] insbesondere bei KMU hingewiesen und auch in den darauffolgenden Studien bestätigt.[111]

Einige **Hemmnisse** für das Erreichen eines entsprechenden IT-Sicherheitsniveaus sind der damit verbundene Kostenaufwand, fehlende Akzeptanz bei den MitarbeiterInnen, kein direkt erkennbarer Vorteil oder Nutzen, fehlende Qualifikation der MitarbeiterInnen, fehlendes Personal, Zeitaufwand, keine Notwendigkeit zur Erhöhung der IT-Sicherheit, Unübersichtlichkeit der vorhandenen Angebote und die Abwesenheit verfügbarer Lösungen.[112] Vielen Unternehmen ist nicht klar, wie mit Schutzleistungen bestehenden Bedrohungen angemessen begegnet werden soll.

Häufig fällt IT-Sicherheit bei kleineren Unternehmen in den Zuständigkeitsbereich der Geschäftsleitung. Laut dem *DsiN Praxisreport 2020* ist die Geschäftsleitung bei 45% der Unternehmen mit unter 10 MitarbeiterInnen für die IT-Sicherheit verantwortlich, während dies bei nur 6% der Unternehmen mit 201 bis 500 MitarbeiterInnen der Fall ist.[113] Kleinst- und Kleinunternehmen schätzen die Risiken Opfer eines Cyberangriffs zu werden tendenziell etwas geringer ein, da sie glauben, dass ihr Unternehmen zu klein sei um für Cyberkriminelle interessant zu sein.[114] Generell scheint sich allerdings unter KMU die Erkenntnis durchgesetzt zu haben, dass die Anzahl von Cyberangriffen in Zukunft eher zunehmen wird.[115]

Dass die erwartete Zunahme von Cyberangriffen nicht nur auf einem Bauchgefühl beruht, bzw. durch das subjektive Sicherheitsempfinden beeinflusst wird, zeigen die Zahlen des *Bitkom Studienberichts 2020*. Demnach waren 88%[116] (79% betroffen und 9% vermutlich betroffen) der kleinen Unternehmen (10-99 MitarbeiterInnen) in den Jahren 2017 und 2018 von Spionage, Sabotage oder Datendiebstahl betroffen.[117] Vor diesem Hintergrund bestätigt der *Bitkom* die eingangs aufgestellte Vermutung, dass KMU als Einfallstor genutzt werden, um sich Zugang zu den über die Lieferketten verbundenen großen Konzerne – die generell besser geschützt sind – zu verschaffen bzw., dass es Cyberkriminelle

[106] Vgl. BSI 2017b, 40.
[107] Vgl. DsiN 2018, 6.
[108] Vgl. DsiN 2020, 28.
[109] Vgl. Bitkom 2018a, 38.
[110] Vgl. BSI 2011, 99.
[111] Vgl. Wik 2017, 52; & it-sa 2014, 5.
[112] Vgl. it-sa 2014, 23; Mijnhardt et al. 2016, 106.
[113] Vgl. DsiN 2020, 19.
[114] Vgl. GDV 2018, 8.
[115] Vgl. Bitkom 2019b, 10. Insgesamt 82% der Unternehmen mit 10-99 MitarbeiterInnen, 78% mit 100-499 MitarbeiterInnen und 80% mit 500 oder mehr MitarbeiterInnen glauben, dass Cyberangriffe stark oder eher zunehmen werden.
[116] Gesamt: 75% betroffen und 13% vermutlich betroffen; n=1.070.
[117] Vgl. Bitkom 2020b, 8.

auf das Spezialwissen der KMU abgesehen haben.[118] Die Studie zeigt aber auch, dass große Unternehmen (ab 500 MitarbeiterInnen) in Deutschland nach wie vor im Fokus von Cyberkriminellen stehen und im Vergleich zur Erhebung aus dem Jahr 2015 einen Anstieg von 24%, bzw. im Vergleich zu 2017, einen Anstieg der Angriffe von 18% verzeichnen.[119] Somit ist fast jedes der befragten Unternehmen von Sabotage, Spionage oder Datendiebstahl in der vernetzten Umgebung betroffen. Hierbei wird nur von Cybervorfällen gesprochen die bekannt sind, die Dunkelziffer dürfte weitaus höher liegen.

Die **Branchenzugehörigkeit** und die damit verbundene IT-Affinität haben auch einen Einfluss auf die Investitionsbereitschaft in IT-Sicherheitsmaßnahmen.[120] Handwerksbetriebe und das Gastgewerbe zeigen sowohl im Umsetzungsgrad als auch in der Innovationsbereitschaft niedrigere Werte auf, als beispielsweise Finanz- oder Versicherungsdienstleister.[121] KMU, die in besonders IT-affinen Märkten operieren, haben schon allein aufgrund ihres Arbeitsumfeldes ein umfassenderes Verständnis der IT-Sicherheit als solche, die in weniger digitalisierten Umgebungen wirtschaften. Dementsprechend generiert sich ein Teil der Bereitschaft in IT-Sicherheit zu investieren aus dem Verständnis vorliegender Bedrohungen und den daraus resultierenden Schlussfolgerungen, die eine Notwendigkeit über den Gedanken des *Return on Investment* (ROI) hinaus erkennen.

Aus der Diskrepanz zwischen der Bedeutung von IT-Sicherheit für KMU und der tatsächlichen Umsetzung lässt sich eine Unsicherheit von KMU über bestehende Risiken und angemessene Lösungen ablesen. Diese Unsicherheit ist zum Teil auch mit dem immer noch bestehenden Marktversagen im Cybersicherheits-Bereich aufgrund von asymmetrischen Informationen zu erklären.[122]

Ein besonderer Nachholbedarf scheint bei deutschen KMU im Bereich des Managements von IT-Risiken zu liegen. Das **Management** von IT-Outsourcing und Cloud-Computing ist trotz einer verbreiterten Nutzung laut einer Studie des *VdS* nur schwach ausgeprägt.[123] Dies ist umso verwunderlicher, da der Umgang mit Daten in der Cloud, gerade von staatlichen Diensten, immer wieder Thema in Politik und Medien ist. „Und trotzdem haben nur 33% der Firmen (im Vorjahr: 27%) für das Thema Cloud-Computing notwendige Anforderungen an die Sicherheit definiert. Über konkrete Sicherheitsvorgaben für Outsourcing-Projekte verfügen ebenfalls nur 38% (2018: 33%, 2017: 30%).“[124] Zudem existieren bei weit über der Hälfte der vom *VdS* befragten Unternehmen keine Richtlinien zum Umgang mit einem Sicherheitsvorfall oder ein Wiederaufbauplan nach dem Ausfall kritischer Systeme.[125]

[118] Ebd.
[119] Ebd.
[120] Vgl. GDV 2018, 9.
[121] Vgl. it-sa 2014, 20.
[122] Vgl. Moore 2010, 7-8.
[123] Vgl. Schmitz 2019, Security Insider vom 19.12.2019, https://www.security-insider.de/positiver-sicherheitstrend-bei-kmu-fuer-2019-a-889695/, Zugriff v. 14.02.2020.
[124] Ebd.
[125] Ebd.

Zu diesen strukturellen Schwierigkeiten von KMU kommen **regulatorische Aspekte** hinzu. Die langfristigen Effekte des IT-Sicherheitsgesetzes und des in der Ressortabstimmung befindlichen IT-Sicherheitsgesetzes 2.0, welches auch die Lieferanten stärker berücksichtigen wird, auf die Investitionsbereitschaft und den Umsetzungsgrad von IT-Sicherheitsdienstleistungen in KMU sind derzeit noch nicht absehbar.[126] Was sich jedoch bereits gemäß der *Wik* Studie sagen lässt ist, dass von diesem Gesetz betroffene Unternehmen höhere Investitionen einplanen. Gleichzeitig besteht unter denjenigen Unternehmen, die nicht von konkreten Regulierungsanforderungen betroffen sind, oftmals der Eindruck einer geringeren Gefährdung.[127] Von den kleineren Unternehmen in der *Wik* Studie gibt über die Hälfte an, mit den gesetzlichen Regelungen zum Thema Datenschutz und IT-Sicherheit überfordert zu sein.[128] Die Datenschutz-Grundverordnung (DSGVO) wird von einigen Unternehmen, unabhängig von der Größe, als Belastung empfunden.[129] Die Anforderungen sind jedoch von vielen Unternehmen noch nicht vollständig umgesetzt.[130]

Auch wenn es selten vorkommt, dass Unternehmen nach einer **Regulierung** durch den Staat rufen, so scheint dies in Bezug auf die Cybersicherheit dennoch zuzutreffen. So ergab der *Thales Data Threat Report* 2018, dass Unternehmen die Aktivitäten der Aufsichtsbehörden begrüßen, wenn es um die Sicherung sensibler Daten geht.[131] Laut der *Thales* Umfrage sind 64% der weltweit Befragten der Meinung, dass die Einhaltung von Compliance-Anforderungen eine "sehr" oder "extrem" effektive Methode zur Datensicherheit ist.[132] Dies ist eine mögliche Erklärung dafür, dass laut der *IDG Security Priorities Study* 2018 69% der Unternehmen die Einhaltung von Compliance-Anforderungen als treibende Kraft für ihre Sicherheitsausgaben sehen.[133]

5.5. Wissenslücken zur weiteren Betrachtung in den quantitativen und qualitativen Umfragen

Aufgrund der großen Bedeutung von KMU für die deutsche Volkswirtschaft sind sie Gegenstand zahlreicher wissenschaftlicher und kommerzieller Studien. Auch IT-Dienstleister finden sich in einigen Analysen wieder, was sich aufgrund des dynamischen Wachstums und ihrer Bedeutung im digitalen Transformationsprozess erklärt. Geht es um die Rolle der IT-Dienstleister für die Cybersicherheit von KMU, so wird der Fundus an Literatur und Studien deutlich dünner.

Die *it-sa* Studie ist unseres Wissens nach eine der wenigen Studien, die sich mit der Angebotsseite kleinstrukturierter IT-Dienstleister beschäftigt. Allerdings ist die Studie von 2014 schon etwas veraltet, hat einen regionalen Fokus und

[126] Vgl. WifOR 2019, 19.
[127] Vgl. Wik 2017, 28.
[128] Ebd., 33.
[129] Vgl. Capgemini 2019, 24.
[130] Ebd., 35.
[131] Vgl. Thales 2018, 18.
[132] Ebd., 15.
[133] Vgl. IDG 2018, 2.

ist nicht repräsentativ. Dagegen ist die Nachfrageseite der KMU, insbesondere durch die *Wik* Studie, schon deutlich besser erforscht.

Es gibt eine Vielzahl von Reports auf internationaler Ebene, die explizit auf die Notwendigkeit von Cybersicherheit für KMU hinweisen. Beispiele sind der *Cisco SME Report 2018*, der *Chubb Australia Cyber Preparedness Report 2018* mit Fokus auf KMU, der *KPMG Cyber Security Guide for SMEs 2016*, oder der *Senseon Report 2019*. Tatsächlich bestätigen diese Berichte den derzeitigen Erkenntnisstand:

1. KMU sind genau wie große Unternehmen von Cyberangriffen bedroht.[134]
2. KMU verfügen über zu begrenzte Mittel (finanzielle Ressourcen, Humankapital, technische Expertise), um angemessen auf Bedrohungen zu reagieren.[135]
3. Angesichts der Komplexität des Bereichs herrscht in der Regel ein großer Beratungsbedarf.[136]

Da die IT-Sicherheitsdienstleister auf direktem oder indirektem Wege immer wieder auf ihre Lösungen verweisen, wie z.B. auf Künstliche Intelligenz (KI) gestützte Cybersicherheit oder Cyberversicherungen, darf man gleichwohl das kommerzielle Interesse nicht ignorieren. Somit müssen Studien, die von IT- und Cybersicherheitsunternehmen verfasst werden, mit etwas Vorsicht betrachtet werden, da diese Unternehmen zum einen ein kommerzielles Interesse verfolgen und zum anderen nur eine ggf. verzerrte Betrachtung, meist basierend auf anonymisierten Kundendaten, des Spektrums zulassen.

Die vorangegangene Analyse zielte darauf ab, den Wissenstand systematisch darzustellen. Im Zuge dessen wurden aber auch einzelne Wissenslücken identifiziert, die mithilfe einer nachfolgenden Befragung der IT-Dienstleister einerseits und ihrer kleinen und mittelgroßen Kunden andererseits, zumindest ein Stück weit, geschlossen werden sollen. Diese Wissenslücken werden im Folgenden kurz skizziert.

5.5.1. IT-Dienstleister / Anbieter

Zunächst einmal wird in der Literatur selten eine klare Unterscheidung zwischen allgemeinen IT-Dienstleistern auf der einen und spezialisierten IT-Sicherheitsdienstleistern auf der anderen Seite vorgenommen. Völlig unklar ist, ob IT-Dienstleister ihren Kunden IT-Schutzmaßnahmen von sich aus empfehlen und somit in den Markt drücken (***push***) oder ob dies nur auf Nachfrage der Kunden erfolgt (***pull***). Sind es die Dienstleister, die das Thema Cybersicherheit vorantreiben, dann stellt sich in der Folge die Frage, auf welcher Grundlage spezifische Maßnahmen angeboten werden. Erfolgt dies auf einer systematischen Risikoanalyse, aufgrund von Veränderungen der Bedrohungslage, oder aufgrund

[134] Vgl. Chubb 2018, 12.
[135] Vgl. Cisco 2018, 7.
[136] Vgl. Senseon 2019, 4.

der vorhandenen Fähigkeiten des Dienstleisters? Wann sehen die allgemeinen IT-Dienstleister überhaupt die **Notwendigkeit, auf IT-Sicherheit spezialisierte Unternehmen zu einem Kundenauftrag hinzuzuziehen**?

Aus welchen Quellen ziehen IT-Dienstleister die Informationen über neue oder sich verändernde Bedrohungen sowie neue Möglichkeiten des Schutzes vor Cyberangriffen? Nutzt man hierzu staatliche Stellen, Messen oder Unternehmensverbände? Zu diesen, in unseren Augen wichtigen, Aspekten der Cybersicherheit konnten wir in den ausgewerteten Quellen keine befriedigenden Antworten finden.

Überhaupt wird bei den IT-Dienstleistern nicht unterschieden, ob diese eigene Sicherheitslösungen für ihre Kunden entwickeln und sich dabei von deren spezifischer Bedrohungssituation leiten lassen, oder ob es sich bei dem Dienstleister eher um eine Vertriebsorganisation handelt, die Lösungen Dritter auf ihre Kunden anpasst. In diesem Zusammenhang ist ebenfalls nicht immer klar, wie sehr bei den Dienstleistern **Branchenwissen** über ihre Kunden notwendig ist, und sich daraus eine Spezialisierung auf Kunden einer bestimmten Branche ergibt. Zwar hat die *Lünendonk* Studie die Notwendigkeit von Branchenwissen für die untersuchten IT-Dienstleister angemerkt - um entsprechende Produkte anbieten zu können ist ein gewisses Branchenwissen abhängig vom Zielmarkt erforderlich - jedoch ist die Frage, wie sich dies bei kleineren Anbietern darstellt. Ist Branchenwissen kein Wettbewerbskriterium, dann stellt sich die Frage, ob die IT-Dienstleistungen nur regional angeboten werden und wie ein entsprechendes Angebot in der Peripherie aussieht. Hierzu konnten keine Informationen gewonnen werden.

Bei der Auswertung der vorhandenen Quellen wird deutlich, dass es sich bei IT-Dienstleistungen um einen sogenannten Anbietermarkt handelt. Wie die Dienstleister zu ihren (neuen) Kunden kommen, bleibt dabei offen. Ganz ohne **Akquisition** und Vertrieb wird es auch hier nicht gehen. Wer sind die Ansprechpartner bei den potentiellen Kunden, welchen Wissensstand besitzen sie, wenn sie die Entscheidung für einen Dienstleister und in der Folge für spezifische Dienstleistungen und Produkte fällen? Wie sehr nutzen die IT-Dienstleister bei der Akquisition, oder auch den Bestandskunden, bestehende staatliche Förderinstrumente?

Immer wieder wird in den Studien und in der Literatur der hohe und weiter zunehmende Mangel an qualifizierten MitarbeiterInnen im Bereich der IT und besonders der IT- und Cybersicherheit bemängelt. Gleichwohl ist über das **Qualifizierungsniveau** bestehender MitarbeiterInnen und Aktivitäten in der Weiterbildung in diesem sehr dynamischen Umfeld wenig bekannt.

Zusammengefasst lassen sich folgende Wissenslücken auf Seiten der IT-Dienstleister / Anbieter feststellen:

- Push- oder Pull-Faktoren bei IT-Schutzmaßnahmen
- Grundlagen für Zusammenstellung des Produktportfolios (Fähigkeiten, Bedrohungslage, etc.)
- Arbeitsorganisation/-prozesse in der Zusammenarbeit mit Dritten (IT-/Cybersicherheitsunternehmen) „im Auftrag“ von KMU
- Informationsgewinnung/Quellen zu Bedrohungslagen

- Notwendigkeit von Branchenwissen bei kleinen IT-Dienstleistern
- Vorgehen bei der Kundenakquisition
- Qualifizierungsniveau der MitarbeiterInnen und Aktivitäten der Weiterbildungsmaßnahmen

5.5.2. KMU / Nachfrager

Da in der Regel eine Unterscheidung zwischen IT-Dienstleistern als Allrounder bzw. Generalisten und IT-Sicherheitsdienstleistern/-unternehmen nicht vorgenommen wird, ist in der Konsequenz auch wenig bekannt, ob KMU IT-Dienstleistungen lieber aus einer Quelle beziehen wollen, oder für spezielle Dienstleistungen Unternehmen bevorzugt werden, die hier einen expliziten Konkurrenzvorteil aufweisen. Dass bei dieser Frage auch ein Zusammenhang zur individuellen Bedrohungslage besteht, liegt auf der Hand, ist aber dennoch nicht empirisch belegt. Überhaupt liegen die Auswahlfaktoren für einen IT-Dienstleister im Dunkeln. Wie bedeutsam ist die regionale Nähe des Dienstleisters? Sind staatliche Regulierung, Standardisierungen, Förderinstrumente, Verbandsinitiativen oder Informationen über die Bedrohungslage Entscheidungsfaktoren, wenn es darum geht auszuwählen, wer für die IT-Sicherheit in einem KMU als Dienstleister herangezogen wird?

Auf welchem Wege, wenn überhaupt, informieren sich KMU über die Bedrohungslage oder werden ihnen diese Informationen zugetragen? In diesem Zusammenhang stellt sich auch die Frage, ob es Kommunikationskanäle und Plattformen des Austausches von KMU mit Kontaktstellen/IT-Dienstleistern gibt, ob sie auf professioneller Ebene ablaufen oder es nur einen informellen Austausch gibt?

Zudem ist nicht immer ersichtlich, wer die Entscheidung bei der Auswahl des IT-Dienstleisters (hierarchische Entscheidungsebene) trifft, und auf welcher Basis dies geschieht. Hat diese Person hinreichendes Wissen, um die unterschiedlichen Angebote qualifiziert beurteilen zu können? Auch die über die Entscheidung der für IT-Sicherheit zur Verfügung stehenden Budgetgröße herrscht weitgehend Unklarheit. In der Folge ist ebenfalls offen, wie die Verteilung des Budgets auf verschiedene Schutzmaßnahmen erfolgt.

Der Mangel an qualifiziertem IT-Personal für die Digitalisierung der Wertschöpfungsketten von KMU ist ein reichlich analysiertes Thema. Inwieweit dieser Mangel dazu führt, Digitalisierungsprojekte, die eigentlich intern durchgeführt werden sollten, an Dienstleister (*Outsourcing*) zu vergeben (und dort für ein entsprechendes Wachstum zu sorgen), ist nicht untersucht. Ebenso stellt sich die Frage, ob der Mangel an Humankapital dazu führt, dass die IT-Sicherheit unzureichend und damit eine Bremse für die Digitalisierung in der Wirtschaft ist.

Diesen Fragen werden wir mit der qualitativen und quantitativen Befragung von IT-Dienstleistern und KMU im nächsten Schritt nachgehen.

Zusammengefasst lassen sich folgende Wissenslücken auf Seiten der KMU / Nachfrager feststellen:

- Auswahlfaktoren für einen IT-Dienstleister (Preis, Qualität, Regionalität etc.)
- Rolle von Standards und Förderprogrammen für die IT-Sicherheit und die Auswahl der IT-Dienstleister
- Informationsbeschaffung zur Bedrohungslage
- Kommunikationskanäle/Plattformen für den Austausch/Kontaktpunkte mit IT-Dienstleistern
- Entscheidungsprozesse und hierarchische Entscheidungsebene
- Entscheidungsprozess des IT-Sicherheitsbudgets
- Einfluss des Fachkräftemangels auf Outsourcing-Entscheidungen

6. Befragung der IT-Dienstleister

Zunächst wurden die Rahmenbedingungen für die Befragung der IT-Dienstleister erarbeitet. Die übergeordneten Fragestellungen für die Befragung der IT-Dienstleister wurden definiert, die Vor- und Nachteile verschiedener Befragungstechniken erörtert und die Samplegrößen festgelegt. In den nachfolgenden Kapiteln werden die Festlegungen erläutert.

6.1. Erarbeitung eines Interviewleitfadens

Aus den Erkenntnissen der Marktbetrachtung ergaben sich Leitfragen, die in die Erstellung des Interviewleitfadens für die Befragung der IT-Dienstleister eingeflossen sind. Anschließend wurden die Evaluationsergebnisse der Pretests dafür herangezogen, den Interviewleitfaden weiter zu präzisieren, zu überarbeiten und nachfolgend für die qualitative Befragung von IT-Dienstleistern verwendet.

6.2. Qualitative Befragung der IT-Dienstleister

Um die Befragten in ihren Antworten nicht zu beeinflussen, wurden offene Interviews geführt und der Interviewleitfaden lediglich als Gesprächsleitfaden verwendet. Die interviewten IT-Dienstleister wurden aus persönlichen Kontakten des Studienteams und aus bundesweiten IHK-Adressbeständen adressiert sowie aus relevanten Netzwerken recherchiert. Die Befragungen erfolgten zunächst (bis einschließlich 14.03.2020) persönlich vor Ort. Aufgrund der COVID-19-Pandemie wurde im laufenden Prozess größtenteils auf eine telefonische Durchführung umgestellt.

Die qualitative Befragung wurde den IT-Dienstleistungsunternehmen wie folgt vorgestellt:

> *Im Auftrag des Bundeswirtschaftsministeriums führen wir eine Studie zur IT-Sicherheit im Bereich der kleinen und mittleren Unternehmen in Deutschland durch. Ziel der Studie ist es, eventuell bestehende Lücken in der Kommunikation zwischen Dienstleistern und potenziellen Kunden zu schließen und somit für mehr IT-Sicherheit am Standort Deutschland zu sorgen.*

Ziel der Interviews war es, neben der Erfassung der Interviewergebnisse, die Entwicklung eines standardisierten Fragebogens zur schriftlichen, online-basierten Befragung einer größeren Menge von IT-(Sicherheits)-Dienstleistern in Deutschland abzuleiten. Dazu wurden nach einem systematischen Quotenplan ost- und westdeutsche, aus ländlichen bzw. Ballungsgebieten stammende, kleinste, kleine und mittelgroße Anbieter von IT-Sicherheitsprodukten und -dienstleistungen befragt (siehe Abschnitt 4.1). Neben statistischen Daten wie Name, Alter, Größe und Sitz(e) des Unternehmens waren folgende Punkte im Fokus der Interviews:

1. Wahrgenommene (IT-)Bedrohungen und Risiken der IT-Sicherheit von KMU aus Sicht der IT-Dienstleister
2. Produktportfolio und technische Lösungen der IT-Dienstleister

3. Arbeitsorganisation und -prozess in der Zusammenarbeit mit bzw. im Auftrag von KMU
4. Qualifikation und Weiterbildung der MitarbeiterInnen der IT-Dienstleister
5. Marketing- und Vertriebsmaßnahmen der IT-Dienstleister

Nach diesen Punkten gliedert sich auch diese Auswertung, die um eine offene Abfrage weiterer interessanter Punkte im Bereich IT-Sicherheit für KMU in Deutschland ergänzt wird.

Die Gespräche wurden zur Datensicherung und für die Auswertung doppelt aufgezeichnet, es gab keinen Widerspruch dazu. Die folgende Auswertung basiert auf 24 (Teil-)Interviews. In einem Fall wurden Interviews für zwei regionale Ausrichtungen mit einem Ansprechpartner geführt.

Inhaltlich befasste sich die qualitative Befragung mit der Einschätzung der IT-Dienstleister zu den folgenden Faktoren:

- Mensch
- Technik
- Organisation
- Erfahrungen mit und Kenntnisse zu Angriffen
- Region
- Branche
- Outsourcing

Die Ergebnisse wurden anschließend als Basis zur Generierung des Online-Fragebogens für die quantitative Befragung von über 100 weiteren IT-Dienstleistern[137] herangezogen. Der qualitative Interviewleitfaden für die IT-Dienstleister wurde inhaltlich mit dem Auftraggeber abgestimmt und von diesem freigegeben.

6.3. Generierung eines quantitativen Online-Fragebogens

Wie bereits im vorigen Abschnitt erläutert, wurden aufbauend auf den Erkenntnissen der offen geführten Interviews die Leitfragen in einen standardisierten Online-Fragebogen überführt. Der Befragungslink wurde an MultiplikatorInnen (siehe Tabelle 6) und an direkte Adressbestände des Studienteams elektronisch versandt. Die Rücklaufquote wurde über den Befragungszeitraum wöchentlich verfolgt. Rücklaufsichernde Maßnahmen, wie Nachfassaktionen und ggf. Telefonbefragungen wurden zur Qualitätssicherung ebenso eingeplant, wie Pretests der Instrumente. Der quantitative Online-Fragebogen für die IT-Dienstleister wurde inhaltlich mit dem Auftraggeber abgestimmt und von diesem freigegeben.

[137] Eine Druckansicht des quantitativen Online-Fragebogens ist dem Anhang zu entnehmen.

6.4. Quantitative Befragung der IT-Dienstleistern

Für die quantitative Befragung der IT-Dienstleister wurde ein Online-Fragebogen (siehe Abbildung 9) generiert, der auf der Projektseite der NKMG mbH veröffentlicht wurde[138].

Abbildung 9 – Startansicht des Online-Fragebogens für die quantitative Befragung der IT-Dienstleister,

DOI: https://www.soscisurvey.de/BefragungITDienstleister/

Um die Bekanntmachung sicherzustellen und die Teilnahmebereitschaft an der Befragung zu erhöhen, hat das BMWi dem Konsortium ein Begleitschreiben ausgestellt, welches dem Anhang (11.6) beigefügt ist.

Für die Veröffentlichung und Verteilung des Online-Befragungslinks bediente sich das Konsortium der Unterstützung verschiedenen Multiplikatoren, die in Tabelle 6 aufgelistet sind. Ein vollständiges Clipping ist dem Anhang (siehe PDF Anhang) zu entnehmen.

[138] Veröffentlichung der Online-Befragung auf der Projektseite der NKMG, DOI: https://www.nkmg-berlin.de/projekte/befragung-zur-studie-it-sicherheit-des-bmwi

Tabelle 6 Multiplikatoren zur Verteilung des Online-Befragungslinks zur quantitativen Befragung der IT-Dienstleister

Institution (Multiplikatoren) zur Verteilung des Befragungslinks zur IT-Dienstleister-Befragung	
Arbeitskreis Software-Qualität und Fortbildung e.V. (ASQF)	Mittelstand Digital, div. Kompetenzzentren
BITKOM – Arbeitskreis Sicherheitspolitik	NKMG Projektseite[139]
BITKOM – Arbeitskreis öffentliche Sicherheit	Projektträger BMWi DLR
BIGS – Newsletter	Projektträger BMBF – VDI
Berlin Partner für Wirtschaft und Energie	SIBB e.V.
Bremen Digital Media – IT-Sicherheit in der Wirtschaft	Sicherheitsnetzwerk München e.V.
Bundesverband IT-Mittelstand e.V. (BITMI)	Software Cluster Süddeutschland e.V.
DeSIN - Deutschland Sicher im Netz (Transferstelle)	Teletrust e.V.
DIHK (Verteilung an alle IHKs, weitere Veröffentlichungen u.a. IHK Berlin, Leipzig, Cottbus, Stuttgart)	Transferstelle IT-Sicherheit - über Fraunhofer FOKUS
Digitale Wirtschaft Schleswig-Holstein (DiWiSH) Wirtschaftsförderung	Transferstelle IT-Sicherheit im Mittelstand
Hochschule für Technik und Wirtschaft (HTW), Berlin - EXIST Projekt	Wirtschaftsförderungsgesellschaften Brandenburg - WFBB
IBWF Institut e.V.	Wirtschaftsförderungsgesellschaften Berlin (Cluster IKT) - BPWT
Innovatives Brandenburg	Zentralverband der Elektrotechnik und Elektronikindustrie e.V. (ZVEI), Fachbereich Sicherheitssysteme
Innovative Hauptstadtregion	4.0 Kompetenzzentrum Illmenau
iTeam Systemhauskooperation	4.0-Kompetenzzentrums Usability

Die mit dem Auftraggeber vereinbarte Zielstellung wurde auf eine Rücklaufquote von mindestens 100 Unternehmen vereinbart. Im Befragungszeitraum vom 22.04.2020 bis 03.07.2020 haben insgesamt 362 IT-Dienstleister, bei 133 gültigen Rückläufern, an der Online-Befragung teilgenommen, womit die vereinbarte Rücklaufquote übertroffen wurde.

[139] Veröffentlichung des Befragungslinks über die Projektseite der NKMG, https://www.nkmg-berlin.de/projekte/befragung-zur-studie-it-sicherheit-des-bmwi

7. Studienergebnisse aus der qualitativen Befragung der IT-Dienstleister

Ziel der qualitativen Befragungen der IT-Dienstleister war einerseits die direkte Befragung der ausgewählten Interviewpartner und andererseits die Entwicklung von standardisierten Fragebögen zur schriftlichen, online-basierten Befragung einer größeren Menge von IT-(Sicherheits)-Dienstleistern in Deutschland. Bei den qualitativen Befragungen der IT-Dienstleister konnten erste Studienergebnisse identifiziert werden, die in den nachfolgenden Abschnitten aufgeführt werden. Die Befragungsergebnisse sind in die Erstellung des Online-Fragebogens der IT-Dienstleister eingeflossen.

7.1. Studienergebnisse der qualitativen Befragung der IT-Dienstleister

Nachfolgend werden die wesentlichen Ergebnisse der qualitativen Befragung der IT-Dienstleister in den Kategorien

- Wahrgenommene Risiken der IT-Sicherheit von KMU,
- Produktportfolio und technische Lösungen,
- Arbeitsorganisation und -prozesse,
- Qualifikation und Weiterbildung der MitarbeiterInnen,
- Marketingkommunikation / Neukundenakquisition und
- Offene Schlussfrage zusammengefasst.

7.1.1. Wahrgenommene Risiken der IT-Sicherheit von KMU

Der Reifegrad der IT-Sicherheit bei KMU ist nach Aussagen der befragten IT-Dienstleister recht unterschiedlich. Die IT-Affinität der Geschäftsführung hat, vor allem bei kleinen und/oder inhabergeführten KMU, einen entscheidenden Einfluss auf die Investitionstätigkeiten und IT-Sicherheitsmaßnahmen des Unternehmens. Entscheider mit der entsprechenden Awareness sind eher gewillt - trotz nicht sofort erkennbarer ROI Vorteile - in IT-Sicherheit zu investieren. UnternehmerInnen, für die solche Investitionen einen reinen Kostenfaktor darstellen, agieren zurückhaltender. Darüber hinaus sind Branchenzugehörigkeit, die Einbettung in Lieferketten und rechtliche Vorgaben weitere Faktoren, die auf den Reifegrad der IT-Sicherheit Einfluss haben. Das IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen und deren Zulieferer sei hier nur beispielhaft erwähnt.

Die befragten deutschen IT-Dienstleister sehen tendenziell eher kleinere und/oder inhabergeführte KMU als stärker bedroht an. Gründe dafür werden vor allem in drei Bereichen gesehen:

(1) Auch kleine KMU sind aufgrund ihrer erheblichen unternehmerischen Bedeutung, teilweisen Weltmarktführerschaft und den damit verbunden wertvollen Informationen in sehr spezifischen Bereichen, ein Angriffsziel für Industriespionage.

(2) Die Angriffe scheinen sich zu professionalisieren. In direkter Ansprache und Form sind Angriffe heutzutage deutlich professioneller und somit schwerer mit einfachen Mitteln zu entdecken. Dies gilt vor allem für Unternehmen, die keine oder nur rudimentäre IT-Sicherheitsmaßnahmen und zentrale Systeme implementiert haben und die z.B. nicht durch eine Netzwerksegmentierung der IT-Infrastruktur getrennt sind. Dies macht es Eindringlingen leicht, das komplette Netzwerk zu übernehmen. Dennoch sind die meisten Angriffe immer noch allgemeinerer Natur und nicht zielgerichtet. Die Angriffsarten (z.B. Ransomware und Phishing in Form von E-Mail-Anhängen mit versteckter Schadsoftware in Word- und Outlook-Macros) scheinen sich nach Angabe der befragten IT-Unternehmen bisher wenig verändert zu haben.

(3) Die Selbsteinschätzung der Bedrohungslagen der KMU scheint sich nach Angaben der befragten IT-Dienstleister teilweise problematisch zu gestalten. Es gibt Unternehmen, die von ihrer (geringen) Größe immer noch auf eine (geringe) Risikolage schließen. Zum Teil berichten die Befragten von einem gewissen Ohnmachtsgefühl bei den KMU: „Ich kann ja eh nichts machen, also lebe ich mit eventuellen Schäden und mache weiter!“

Aus Sicht der befragten IT-Dienstleister rückt der **Faktor Mensch** als wichtigster Sicherheits- und Risikofaktor in den Fokus, was offenbar mit einer zu geringen Sensibilisierung und/oder zu geringem Wissen um die Gefahren im IT-Bereich oder einfachem „Laissez-faire“-Bewusstsein innerhalb der KMU zusammenhängt. Mit besserer Vorbildung, Fachkenntnis und einem höheren Grad an Awareness und Sensibilisierung wären viele Angriffe an ihrer Natur erkennbar.

Der Faktor Mensch ist nach Angabe der IT-Dienstleister oft direkt mit dem **Faktor Organisation** verknüpft. Selbst wenn eine gewisse Awareness und ein guter technischer Wissensstand vorhanden sind, gibt es in manchen Fällen offenbar große organisatorische Lücken und Risiken: „Server laufen, aber wer hat den Schlüssel zum Raum? Wie ist der Raum gegen Eindringen gesichert? Wer hat welche Zugangsberechtigungen?“ Ein relativ oft genanntes Szenario stellt das Handeln ehemaliger MitarbeiterInnen dar, die Daten, Hard- und Software sowie Zugangsberechtigungen mitnehmen bzw. über die Unternehmenszugehörigkeit hinaus Zugriff auf kritische Daten und Unternehmensbereiche haben.

Auch eine direkte Verbindung des Faktors Mensch zum **Faktor Technik** wird angesprochen, wenn beispielsweise technische Sicherheitsprotokolle geschrieben werden, aber niemand die Speicherung und Ablage kontrolliert oder wenn Back-ups nicht entkoppelt erstellt werden.

Konkrete Erfahrungen mit Angriffen bei KMU-Kunden hatten alle befragten Unternehmen, je nach Ausrichtung des IT-Dienstleisters als Servicedienstleister oder als Notfallhilfe, intensiver oder weniger intensiv. In den Erfahrungen der befragten IT-Dienstleister lagen ganz selten direkte Angriffe vor, einige mittlere und größere KMU waren von Verschlüsselungserpressungssoftware betroffen. Die häufigsten Vorfälle gab es nach Angabe der befragten IT-Dienstleister durch Emotet und infizierte Office- und Outlookdokumente. In Unternehmen, in denen nur kleinere kaufmännische Abteilungen bestehen, sofern überhaupt vorhanden, wurden offenbar z.T. Fake-Rechnungen ohne Überprüfung (aufgrund von Überlastung) bezahlt.

Der **Faktor Region** wird für die Nachfrage und das Angebot der Dienstleistungen von fast allen befragten IT-Dienstleistern nicht als ausschlaggebend angesehen. Ausnahmen sind ein, von einzelnen Befragten angegebenes, Mehr an Austausch über Angriffe und Bedrohungen in Ballungsräumen. Eine regionale Besonderheit stellen besondere Konkurrenzsituationen auf dem Arbeitsmarkt dar, wenn große Unternehmen mit hohen (Einstiegs-)Gehältern, zumeist in Ballungsräumen, den IT-Dienstleistern das Recruiting erschweren.

Der **Faktor Branche** spielt eine besondere Rolle und wird durch die Befragten fast durchgängig bestätigt. Produzierendes Gewerbe hat oftmals kaum Kapazitäten, sich neben der für den Betrieb essentiellen Produktions-IT noch auf andere Bereiche zu konzentrieren. Etwas anders sieht es insbesondere im Bereich Kritischer Infrastrukturen und bei KMU aus, die in Zulieferketten für Großunternehmen tätig sind. Dort scheint es nach Angaben der befragten IT-Dienstleister eine größere Awareness für IT-Sicherheitsbedarfe zu geben. In diesen Fällen ist es weniger schwierig, die benötigten Ressourcen (Budget und Verantwortlichkeit) freizusetzen. Zeitmangel und „Nicht-Sichtbarkeit“ von Datenverlusten sowie Mangel an Grundverständnis für die ablaufenden Prozesse führen immer wieder zu großen Sicherheitslücken in allen Branchen. Nur fortwährendes Nachhalten gewährleistet ein höheres Niveau an Sicherheit.

7.1.2. Produktportfolio und technische Lösungen

Die Produktportfolios der befragten IT-Dienstleister sind recht unterschiedlich und könnten auf eine stark fragmentierte Anbieterlandschaft hindeuten. Unter den befragten IT-Dienstleistern finden sich reine Beratungsunternehmen, die sich noch einmal aufteilen lassen in Notfalldienstleister, Awareness- und Organisationsmanagementberater sowie Risikoprüfer, Gutachter, Zertifizierungsberater und Auditoren. Manche der befragten Beratungsfirmen unterstützen dies mit eigens entwickelten Software- oder Hardwarekomponenten, die für bestimmte Bereiche der KMU entwickelt wurden, z.B. Applikationen (Apps) zum *Onboarding* von Zulieferern oder Handwerkern, *AppLayer* zur Sicherung externer Endgeräte bei der Verwendung von WhatsApp etc. oder günstige, kleine Überwachungs- und *Monitoringboxen* für Netzwerke. Befragte Firmen mit kompletter Notfallhilfe, Forensik, einer Einbindung von Landeskriminalämtern (LKA) bei gemeldeten Ereignissen und Kooperationen mit Rechtsanwälten arbeiten eher ab relativ hohen Umsätzen der KMU ganzheitlich.

Bei den befragten kleineren Techniklieferanten wird zumeist mehr Wert auf Expertise und Perimetersicherheit gelegt. Der BSI-Grundschutz, weitere Standards und Zertifizierungen zur Informationssicherheit werden allgemein auf die Kundengröße angepasst. Oft sind die existierenden Standards in ihrem gesamten Umfang nur schwer im KMU-Kundensegment vermittelbar. Die Portfolios der befragten Unternehmen beinhalten zum großen Teil auch Beratung und Service.

Die befragten Systemhäuser widmen sich am wenigsten dem spezifischen Anpassen von Technik und Organisation auf die jeweils besonderen KMU-Strukturen. Ihr Interesse gilt mittleren und größeren KMU, um möglichst wirtschaftlich

zu arbeiten und Entwicklungskosten durch Vervielfältigung der Services zu reduzieren (skalierbare Modelle). Vereinzelt unterstützen sie KMU in und bei Förderprogrammen.

Standardisierte Produkte sind bei fast allen befragten IT-Dienstleistern angestrebt – sogar bei Selbstentwicklern – damit Wartung und Management frei durchführbar und auch ersetzbar bleiben. Das Interesse an technischen Neuerungen und aufkommenden Bedrohungen ist groß und wird besonders durch individuelle, meist Online-Weiterbildung, genährt (abgesehen von reinen Herstellerrepräsentanten).

Für die meisten IT-Dienstleister ist vor allem die Ermittlung des Kerngeschäfts entscheidend und damit die Einschätzung, ob technische Neuerungen im Produktportfolio in skalierbarer Zahl die KMU erreichen. Spezifische Lösungen lohnen sich nur dort, wo sie in dem Einzelfall einen wirtschaftlichen Erfolg generieren oder im Anschluss als skalierbares Produkt mit entsprechendem Nachfragepotential angeboten werden können. Ein großes Wachstumspotenzial in den letzten fünf Jahren ist laut IT-Dienstleistern bei *Network-Access-Control-Systemen*, *AppLayern* und *Awareness*-Schulungen zu beobachten.

Bei Preis-Leistungsdiskussionen gilt nach Auskunft der befragten IT-Dienstleister fast immer, dass Budgets für IT-Sicherheit auf KMU-Seite knapp bemessen sind. Dies verwundert kaum, zeigt jedoch einmal mehr, dass für viele KMU der Preis über Leistung und Qualität steht. Allerdings fehlt oft der Überblick über Fördermöglichkeiten, den Wert des Kerngeschäfts und die Bedeutung einer störungsfrei laufenden Informations- und Kommunikationstechnik.

Weniger Preisdiskussionen gibt es bei Kritischen Infrastrukturen, Zulieferern für große Firmen mit Compliance- und KMU mit eigener IT-Abteilung. Am meisten nachgefragt wird „das Rundum-Sorglos-Paket zum günstigen Preis“ – nicht selten nach einem Schadensfall.

7.1.3. Arbeitsorganisation und Arbeitsprozess

Die meisten der befragten IT-Dienstleister haben feste AnsprechpartnerInnen oder Teams auf ihrer und der KMU-Seite. Beim Dienstleister werden diese oft von Hotlines und Ticketsystemen, außer bei reinen Beraterhäusern, Schulungsanbietern oder sehr kleinen Dienstleistern unterstützt.

Periodisch wiederkehrende Dienstleistungen oder Updates - je nach Vertrag und Bedarf wöchentliche, monatliche, quartalsweise oder jährliche - bieten vornehmlich kleine und mittlere befragte IT-Dienstleister an. *Jour Fixes* üblich, um alle Bereiche kontinuierlich zu kontrollieren und weiter zu planen.

Klein(st)e Unternehmen arbeiten gern in Netzwerken zusammen, so z.B. beim BSI-Grundschutz oder der Verwendung und Weiterentwicklung von *Open Source* Produkten oder *Blockchain*-Technologien. Damit kann internationales Know-how selbst über regionale Kleinstunternehmen in Deutschland flächendeckend weitergegeben und angewandt werden.

Die Zusammenarbeit mit IHK und Handwerkskammer ist nahezu bei allen befragten IT-Dienstleistern durchgesetzt oder angestrebt, läuft aber regional sehr unterschiedlich. Gute Erfahrungen gibt es im Auszubildendenbereich und in einigen Regionen mit der IT-Sicherheitsinformation bezüglich Förderungen und passenden Informationsveranstaltungen.

IT-Dienstleister mit hohem Sicherheitsanteil im Portfolio legen großen Wert darauf, stets „am Puls der Zeit" zu sein und dies auch nach außen darzustellen. Dabei ergibt sich bei den befragten Unternehmen eine gewisse Zweiteilung in FachspezialistInnen (oft universitäre Ausgründungen). Es werden einerseits Software- und technische Lösungen und andererseits nach Analyse der KMU-Kerngeschäfte eine Kombinationslösung aus Technik und Organisation entwickelt. Sie sollen nur so agil und teuer wie nötig sein, um den KMU Kapazitäten für den Betrieb und Ausbau ihrer eigentlichen Produktion zu lassen.

7.1.4. Qualifikation und Weiterbildung der MitarbeiterInnen

Bei Studienabschlüssen nennen die befragten IT-Dienstleister zumeist Fachhochschulen mit Informatik- oder betriebswirtschaftlichen Schwerpunkten, seltener kommen spezifische Abschlüsse der IT-Sicherheit oder ein entsprechendes Universitätsstudium vor. Es ist zu vermuten, dass dies auch der Tatsache geschuldet ist, dass bis jetzt an wenigen Hochschulen spezielle IT-Sicherheitsstudiengänge angeboten werden. Aufkommend sind Kooperationen mit dualen Studiengängen.

BerufsabschlüsseSind vorwiegend FachinformatikerIn, SystemadministratorIn oder SystementwicklerIn. QuereinsteigerInnen aus allen Richtungen mit dem ausgewiesenen Interesse und Entwicklungspotenzial in Sachen IT und IT-Sicherheit werden gern getestet und bei Eignung übernommen.

Bei den befragten IT-Dienstleistern mit bestehenden Bindungen an große Hard- und Softwareunternehmen wird meist der entsprechende Partnerstatus angestrebt, das heißt, MitarbeiterInnen absolvieren regelmäßig die geforderten Schulungen, um die passenden Zertifikate zu erhalten. Diese werden dann auch bereitwillig als Referenzen verwendet.

Herstellerunabhängige Dienstleister bevorzugen die Weiterbildung in passenden nationalen und internationalen Netzwerken mit entsprechenden Konferenzen und Messen, oder organisieren selbst die Weiterbildungen, die für die aktuell laufenden Projekte nötig und hilfreich sind. Diese Unternehmen benutzen ihre Verbands- oder Netzwerkmitgliedschaften (s.u.) oder Firmen, für die erfolgreich gearbeitet wird, oft auch als Referenzen für die angebotene Qualität.

Für die kleinsten befragten Dienstleister trifft davon oftmals nur ein Bruchteil zu, der sich außerdem nur auf wenige Produkte bezieht.

7.1.5. Marketingkommunikation/ Neukundenakquisition

Die befragten mittleren IT-Unternehmen und (auch kleinere) Systemhäuser scheinen zumeist nur Interesse an Kunden ab einer gewissen Größenordnung zu haben. Deshalb schalten sie gezielte Anzeigen, veranstalten oft In-House-Messen und Business-Treffen, verwenden Akquisitionspartner und Ausschreibungsdienstleister. Die Ansprache erfolgt dabei spezifisch unterschiedlich an die Geschäftsführung und IT-Abteilungen der KMU. Webseiten scheinen diese IT-Dienstleister eher allgemein zu gestalten, um z.B. mit Herstellerpartnerschaften und großen Firmenprojekten als Referenzen zu werben. Trotz dieser recht umfangreichen Maßnahmen geben die befragten mittelgroßen IT-Dienstleister an, keine große Mühe bei der Akquisition zu haben.

Unabhängig von der Größe des Unternehmens agieren auf IT-Sicherheit und Datenschutz spezialisierte Dienstleister nach Angaben der in diesem Segment befragten Unternehmen anders. Sie versuchen ihre besondere Expertise in einigen Segmenten durch gezielt zugeschnittene Webseiten, Auftritte auf Fachkonferenzen und –messen, Dozentenjobs an Hochschulen und Universitäten, bis hin zu Professuren, auszuweisen. Diese Unternehmen beteiligen sich an einschlägigen Ausschreibungen und nutzen ihre stark inhaltlich ausgerichteten Mitgliedschaften in Netzwerken.

Fast nur durch „Mund-zu-Mund-Propaganda“ und Handschlag-Referenzen, ergänzt durch Mitgliedschaft in regionalen Verbänden und regelmäßigen Besuchen der ein bis zwei wichtigsten Messen, arbeiten die befragten klein(st)en regionalen „Hands-on“-Dienstleister, ob in Beratung oder technischem Support. Hier ist Vertrauen höchstes Gut. Zertifizierungen spielen nach Angabe der in diesem Segment befragten IT-Dienstleister keine Rolle. Wachstum ist oft nur dann gefragt, wenn sich mithilfe dieses Wachstums eine inhaltliche Portfolioerweiterung ergibt.

Sonderrollen bei der Akquisition und der Marketingkommunikation spielen befragte Erste-Hilfe-ManagerInnen im Schadensfall, die auch als “erste/r Zeuge/ Zeugin agieren” und als BeraterInnen für Sicherheit direkter Produkte (z.B. SAP, Microsoft) fungieren. Einige befragte Unternehmen, die mit großen Erste-Hilfe-Netzwerken (Anwälte, Techniker, Polizei/LKA) zusammenarbeiten, halten – nach Bedeutung und Größe gestaffelte – *Business*-Treffen ab, um in Notfällen schnell und ausreichend freie Fachleute im Netzwerk zu haben.

Oft bestehen bei den befragten IT-Dienstleistern Mitgliedschaften in oder zumindest engste Beziehungen zu Unternehmerverbänden. Häufig wurde der „Verband der Familienunternehmer“ vornehmlich von mittleren Unternehmen und Systemhäusern, die befragt wurden, genannt. Weitere mehrfach genannte Verbände und Netzwerke waren die „Allianz für Cybersicherheit“ oder der „TeleTrusT e.V.“. IHKs scheinen sehr unterschiedlich in ihrer Bedeutung für die Befragten.

Fachkräftemangel herrscht bei den befragten mittleren IT-Dienstleistern neben den o.g. Konkurrenzsituationen vor allem im gehobenen technischen Support und Management sowie bei Senior Consultants im Vertrieb. Befragte Ausbildungsbetriebe geben an, sich den benötigten Nachwuchs selbst heranzuziehen. Einige der befragten Unternehmen locken mit der „bunten Google-Spielelandschaft“ mit Wohnzimmeratmosphäre und gemeinsamen Teamevents im Rahmen von Meetings. Wachstumsabsichten werden von den Befragten nicht einheitlich genannt und mit dem Fachkräftemangel auch nicht einheitlich verbunden.

7.2. Studienergebnisse der quantitativen Befragung der IT-Dienstleister

Nachfolgend werden die wesentlichen Ergebnisse der quantitativen IT-Dienstleister Befragung in den Kategorien

- statistische Daten der Unternehmen,
- wahrgenommene Risiken der IT-Sicherheit von KMU,
- Produktportfolio und technische Lösungen,
- Qualifikation und Weiterbildung der MitarbeiterInnen,
- Marketingkommunikation/Neukundenakquisition,
- Kooperationsplattformen und Netzwerke,
- öffentliche Förderung und
- besondere Hemmnisse zusammengefasst.

7.2.1. Statistische Daten der Unternehmen

An der Umfrage nahmen insgesamt 362 Unternehmen teil. 133 Fragebögen wurden vollständig ausgefüllt. Letztere sind die Grundlage der folgenden Analyse. Die meisten teilnehmenden Unternehmen können dem mit der Umfrage adressierten KMU-Bereich der IT-Dienstleister zugeordnet werden. Nur 2% geben an, mehr als 500 MitarbeiterInnen zu beschäftigen. Den größten Anteil der Befragten machen Kleinunternehmen mit 10 bis 49 MitarbeiterInnen (39%) aus. 12% der Unternehmen haben zwischen 50 und 499 Beschäftigte. Weitere 38% der Unternehmen sind dem Bereich Kleinstunternehmen mit bis zu 9 MitarbeiterInnen zuzuordnen.

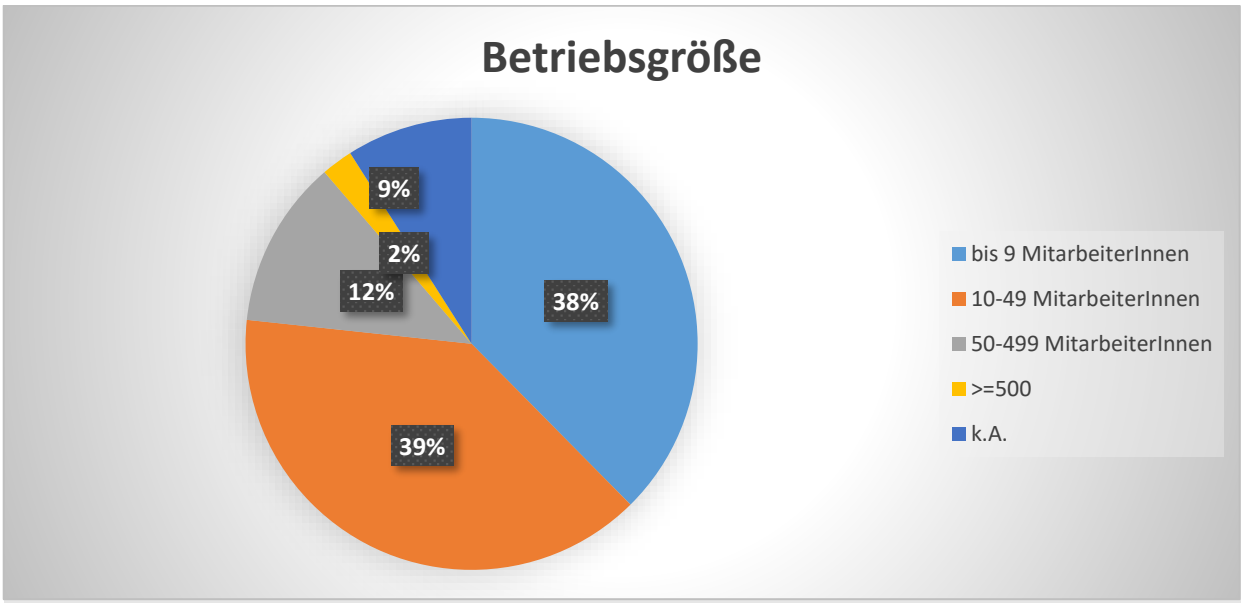

Abbildung 10 – Größe des Unternehmens (Anzahl MitarbeiterInnen in Vollzeitäquivalente).

Die meisten an der Umfrage beteiligten Unternehmen kommen aus Nordrhein-Westfalen (16%), gefolgt von Baden-Württemberg (14%) und Bayern (9%). Insgesamt haben mit 63% mehr Unternehmen aus den „alten“ als aus den „neuen Bundesländer (inklusive Berlin)“ mit 28% an der Umfrage teilgenommen. 9% haben dazu keine Angaben gemacht. Die Anzahl der Unternehmen in den „alten“ Bundesländern beträgt laut Angaben des Instituts für Mittelstandsforschung 2.823.000 (81%) und in den „neuen“ Bundesländer (inklusive Berlin) 667.000 (19%)[140]. Geht man davon aus, dass der Anteil der IT-Dienstleister in beiden Bereichen ähnlich ist, so sind die an der Umfrage beteiligten Unternehmen aus dem Osten überproportional vertreten.

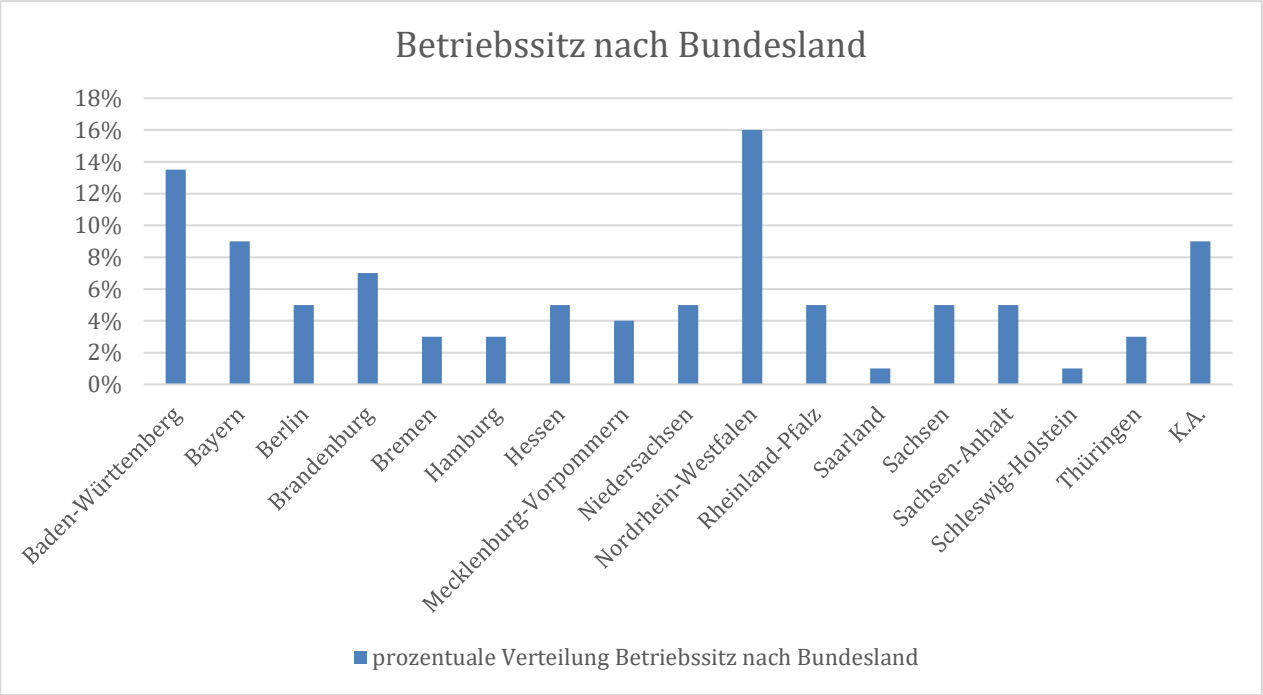

Abbildung 11 – Verteilung nach Hauptbetriebssitz der an der Umfrage beteiligten IT-Dienstleister.

Die an der Umfrage teilnehmenden Unternehmen sind mehrheitlich schon länger in dem Geschäftsfeld tätig und haben somit eine gewisse Branchen- bzw. Markterfahrung (67% seit mehr als 10 Jahren bzw. 35% seit mehr als 20 Jahren). Eine größere Markt- und Branchenerfahrung der IT-Dienstleister sollte tendenziell dazu führen, dass sie die Lage der IT-Sicherheit ihrer Kunden besser einschätzen können.

[140] Berechnet aus den Angaben des Instituts für Mittelstandsforschung (IfM) Bonn: Vgl. https://www.ifm-bonn.org/fileadmin/data/redaktion/statistik/mittelstand_im_einzelnen/dokumente/Unt_2018_D_BL_KMU-Dichte.pdf

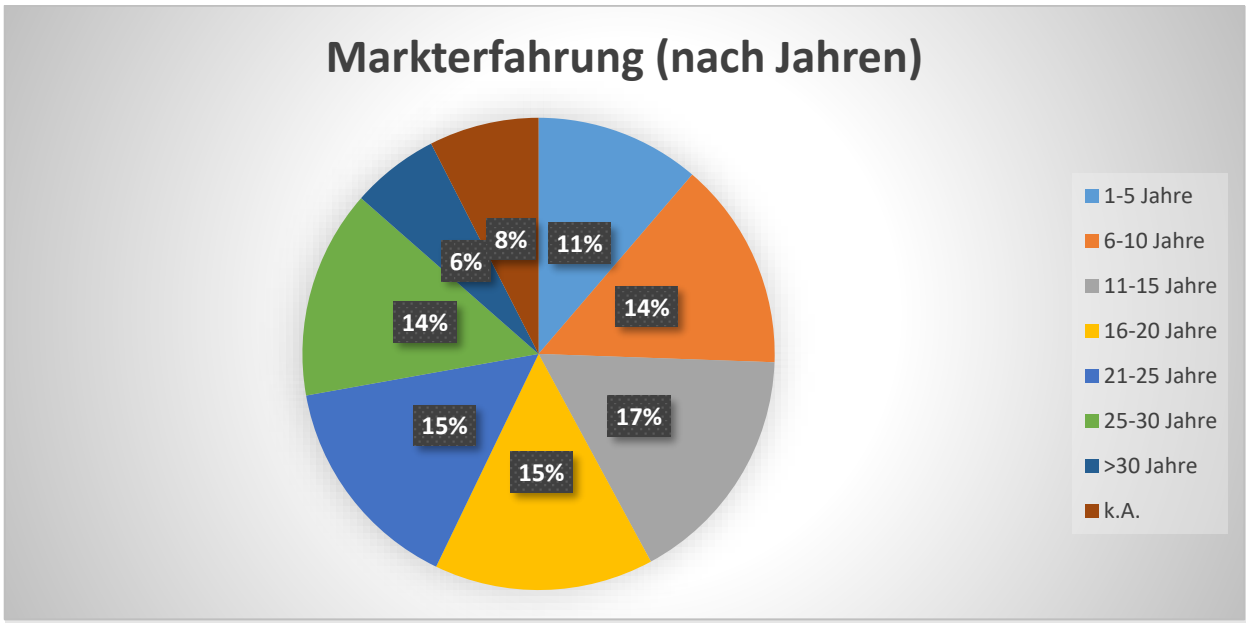

Abbildung 12 – Anzahl Jahre der Betriebstätigkeit des Unternehmens im IT-Dienstleistungssektor.

34% der befragten Unternehmen sind deutschlandweit, 18% in der DACH Region und 14% in der EU bzw. international tätig. Nur 26% gaben an, dass sie ausschließlich in ihrer Region operativ arbeiten. Nach welchen Kriterien die Marktaufteilung vorgenommen wurde, ob das Unternehmen bewusst oder notgedrungen regional oder national operiert, sich in der Konsolidierungs- oder Expansionsphase befindet, lässt sich aus den Antworten nicht ableiten. Es ist aber zu vermuten, dass der zunehmende Fachkräftemangel eine überregionale Ausweitung der Geschäftstätigkeit erschwert.

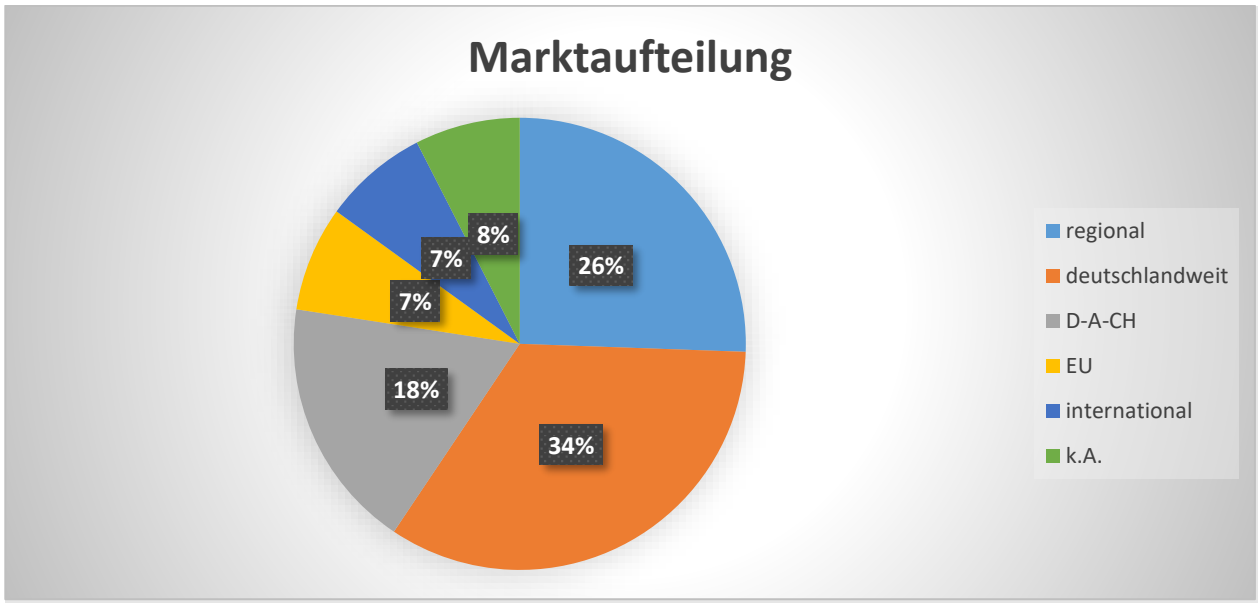

Abbildung 13 – Marktaufteilung der befragten IT-Dienstleistungsunternehmen.

7.2.2. Wahrgenommene Risiken der IT-Sicherheit von KMU

Die BefragungsteilnehmerInnen wurden nach ihrer Einschätzung bzgl. der Eintrittswahrscheinlichkeit von Bedrohungen in den Bereichen Menschliches Versagen (z. B. mangelnde IT-Kenntnisse im Zusammenhang mit Angriffen/Schadsoftware/Phishing etc.), Technisches Versagen (z. B. unzureichender Schutz der IT-Infrastrukturen), Organisationsversagen (z. B. ungenügende Regelungen zu Zugangsmanagement oder Sicherheit von Identitäten) und Angriffe (z. B. Schadsoftware, DDos-Angriffe, etc.) für ihre KMU-Kunden gefragt.

Der Faktor Mensch wird laut TeilnehmerInnen als das größte potentielle Risiko für die IT-Sicherheit von KMU angesehen. So schätzen 55% die Eintrittswahrscheinlichkeit von menschlichem Versagen als sehr hoch und weitere 42% als eher hoch ein. Durch technisches Versagen Opfer eines Cyber-Vorfalls zu werden, gaben lediglich 11% als *sehr hohes* und immerhin 40% der Befragten als *eher hohes* Risiko an. Im Bereich Organisationsversagen waren 25% der IT-Dienstleister der Meinung, dass durch z.B. mangelnde oder unzureichende interne Prozesse ein *sehr hohes* und 40% ein *eher hohes* Risiko besteht. Schließlich wurden Angriffe mit 16% als *sehr hohes* bzw. mit 38% als *eher hohes* Risiko bei der Eintrittswahrscheinlichkeit von Bedrohungen benannt.

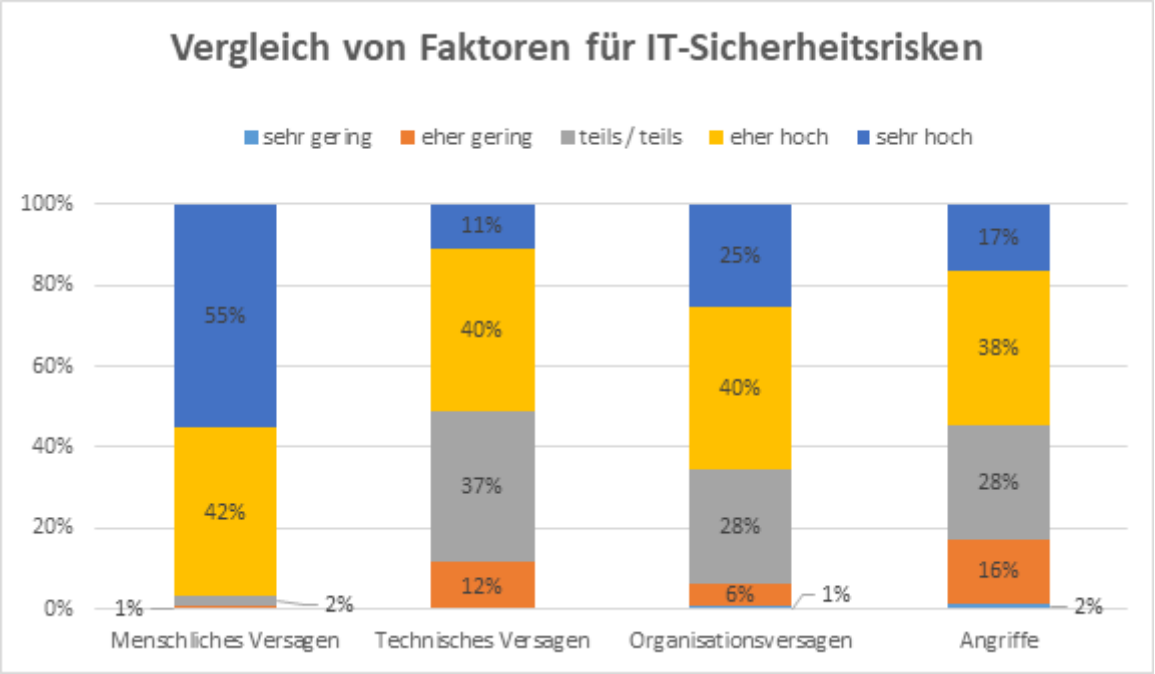

Abbildung 14 – Im Vergleich die Eintrittswahrscheinlichkeiten für die jeweiligen Bedrohungen für KMU aus Sicht ihrer IT-Dienstleister.[141]

Im direkten Vergleich der Antwortmöglichkeiten *sehr hoch* und *eher hoch* mit den anderen Bereichen zeigt sich, dass die IT-Dienstleister die Eintrittswahrscheinlichkeit von menschlichem Versagen am höchsten bewerten. Es folgen Organisationsversagen, Angriffe und zuletzt technisches Versagen.

Diese Aussagen sind keine große Überraschung, zeigen aber einmal mehr, dass der Faktor Mensch nach wie vor eine herausragende Rolle bei der Umsetzung von IT-Sicherheitsmaßnahmen spielt. Dies trifft ganz besonders auf KMU zu, die sich in der Regel weder technisch versierte IT-SicherheitsmitarbeiterInnen noch eine umfangreiche IT-Sicherheitsinfrastruktur leisten. Insofern können die IT-Dienstleister gerade im KMU-Segment zu einer Steigerung der IT-Sicherheitsniveaus beitragen.

Mängel in organisatorischen Prozessen können es Angreifern leicht machen, Sicherheitsvorkehrungen unbemerkt zu überwinden. Im Umkehrschluss können gerade organisatorische Sicherheitsmaßnahmen dazu beitragen, einen höheren Schutz mit einem relativ geringen Budget zu erreichen. Auch hierbei können IT-Dienstleister ihre Fach- und Branchenerfahrung effizient einbringen.

[141] Frage: Nachfolgend sind einige Bereiche aufgeführt, in denen KMU IT-Sicherheitsrisiken ausgesetzt sein können. Bitte geben Sie hier anhand der angegebenen Skala (eher gering, teils/teils, eher hoch, sehr hoch) an, für wie hoch Sie die Eintrittswahrscheinlichkeit für die jeweiligen Bedrohungen in diesem Bereich für Ihre KMU-Kunden einschätzen!

In der folgenden Grafik sind im Vergleich die Antworten der IT-Dienstleister zusammengefasst, die ein *sehr hohes* und *eher hohes* Risiko für menschliches und technisches Versagen, Organisationsversagen sowie für Angriffe bei ihren KMU-Kunden sehen.

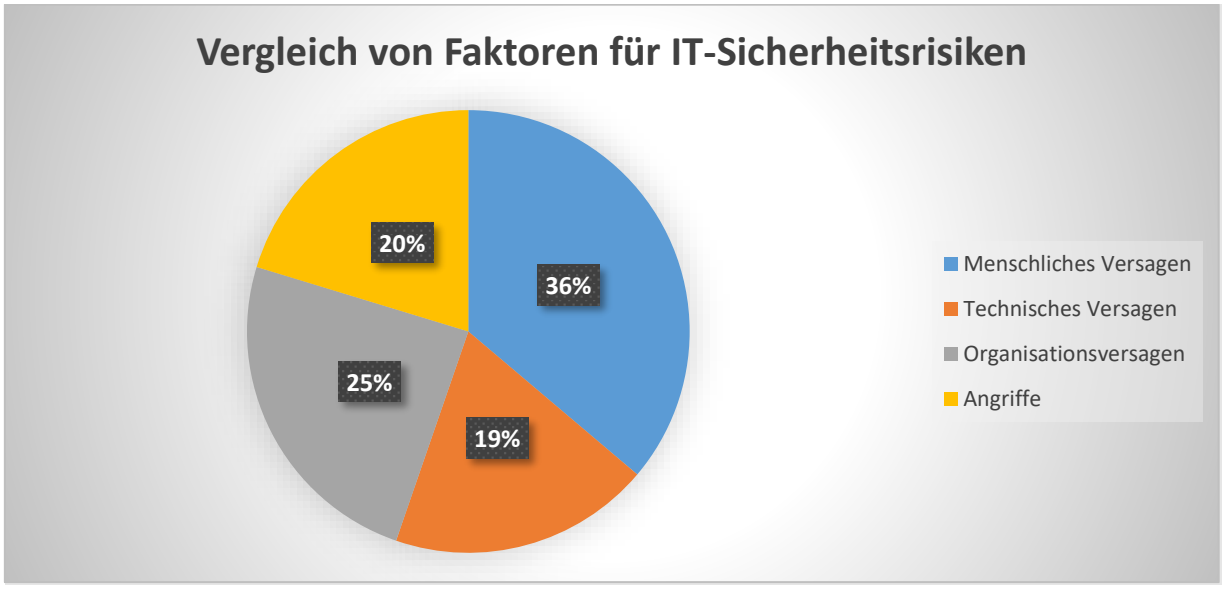

Abbildung 15 – Im Vergleich die Eintrittswahrscheinlichkeiten eher hoch und sehr hoch für die jeweiligen Bedrohungen für KMU aus Sicht ihrer IT-Dienstleister.

In der Bewertung des möglichen bzw. tatsächlich eingetretenen Schadens bei KMU, wird der Schaden durch menschliches Versagen im Vergleich der Faktoren, als am bedeutendsten eingestuft. Bei der Einzelbetrachtung gaben 36% der Befragten an, dass sie menschliches Versagen für einen *sehr großen* sowie 37%, dies für einen *eher großen* Faktor bei möglichen bzw. tatsächlich eingetretenen Schäden halten.[142]

[142] Technisches Versagen: 23% sehr groß, 34% eher groß; Organisationsversagen: 18% sehr groß, 35% eher groß; Angriffe: 19% sehr groß, 32% eher groß (siehe auch alle Auswertungen im Anhang).

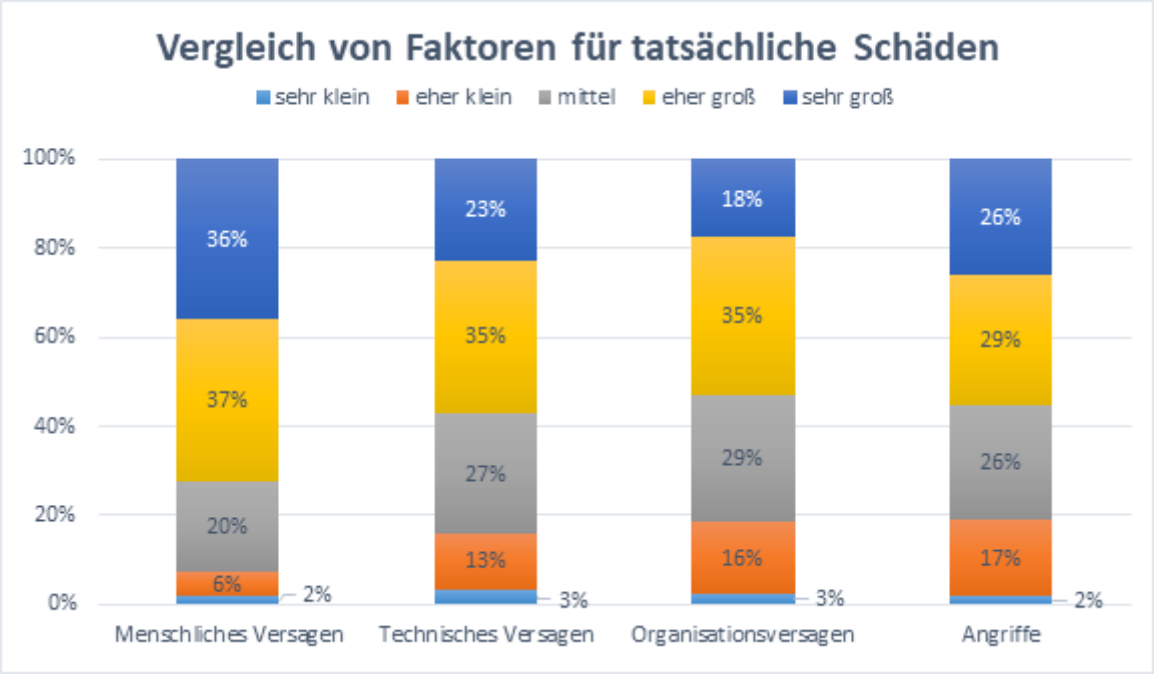

Abbildung 16 – Im Vergleich Bewertung des möglichen bzw. tatsächlich eingetretenen Schadens durch die jeweiligen Bedrohungen für KMU aus Sicht ihrer IT-Dienstleister.

Eine unzureichende Sensibilisierung für das Thema IT-Sicherheit, sowie fehlende Organisationsprozesse und Handlungsmaßnahmen bei Vorfällen führen nach Meinung der befragten IT-Dienstleister zu einem erhöhten Sicherheitsrisiko für die Unternehmen.

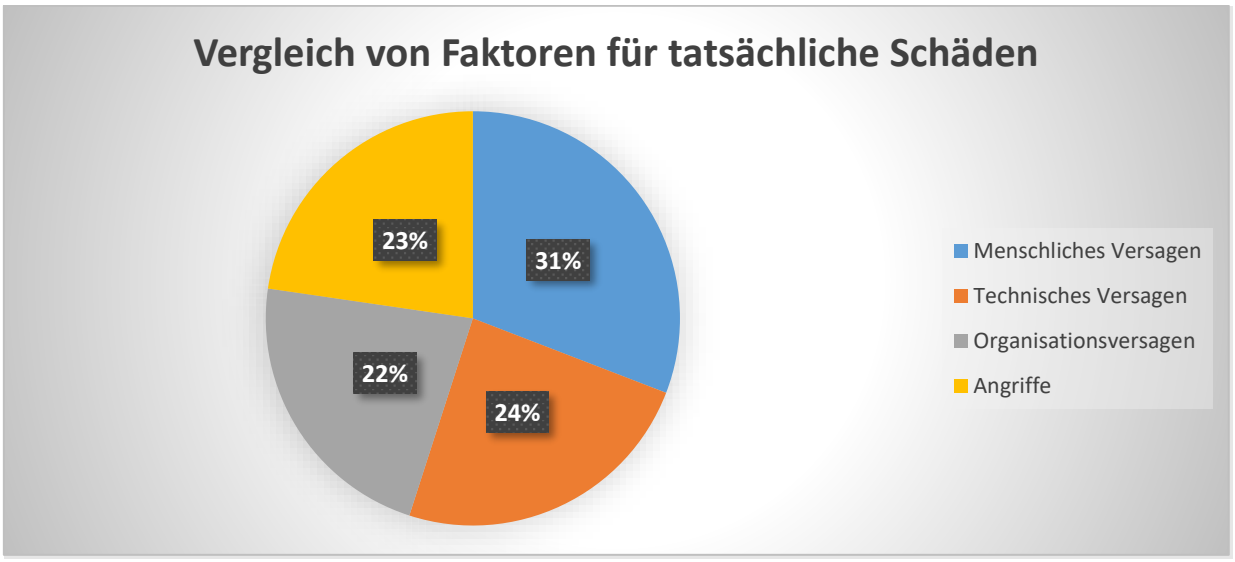

Abbildung 17 – Im Vergleich Bewertung (eher groß bzw. sehr groß) des möglichen bzw. tatsächlich eingetretenen Schadens durch die jeweiligen Bedrohungen für KMU aus Sicht ihrer IT-Dienstleister.[143]

Die Antworten verdeutlichen, dass menschliches Versagen aus Sicht der IT-Dienstleister nicht nur als wahrscheinlichstes IT-Sicherheitsrisiko für KMU angesehen wird, sondern aus ihrer Sicht auch für den größten Schaden verantwortlich gemacht wird.

Awareness und Sensibilisierung für das Thema IT-Sicherheit stehen seit Jahren auf der Agenda von Wirtschaftsverbänden, Politik, Ministerien und Behörden, der Zivilgesellschaft und der Wissenschaft. Dennoch zeigt sich, dass der Faktor Mensch und die damit verbundenen Schwachstellen, nach wie vor eine entscheidende Rolle in der IT-Sicherheitsstruktur spielen. Dies gilt umso mehr in Organisationen, die keine adäquate technische IT-Sicherheitsinfrastruktur vorweisen können. Gründe dafür sind ein Mangel an Know-how, an qualifiziertem Personal und auch fehlende finanzielle Mittel. Konzentrieren sich Prozesse auf einige wenige Knotenpunkte, wird es Angreifern leicht gemacht, mit einfachen (technischen) Mitteln großen Schaden anzurichten.

7.2.3. Produktportfolio und technische Lösungen

Die IT-Dienstleister wurden gefragt, inwiefern sie im Vertrieb und in der Entwicklung der folgenden sechs Technologien tätig sind: 1) Hardware, 2) Software, 3) IT-Infrastruktur, 4) Netzwerktechnologien, 5) Sicherheitstechnologien und 6) ID-Lösungen. Die Antworten zeigen, dass die befragten Unternehmen im Vertrieb mehrheitlich auf hybride Lösungen setzen, also einem Mix aus Standard- und spezifischen Lösungen. Bis auf bei ID-Lösungen (45%), machen diese

[143] Frage: Bitte geben Sie nun anhand der angegebenen Skala (sehr klein, eher klein, mittel, eher groß, sehr groß) an, für wie groß Sie den möglichen bzw. tatsächlich eingetretenen Schaden in diesem Bereich für Ihre KMU-Kunden einschätzen!

hybriden Technologielösungen z.T. weit über die Hälfte des Angebots aus, bei der IT-Infrastruktur sogar zwei Drittel (64%).

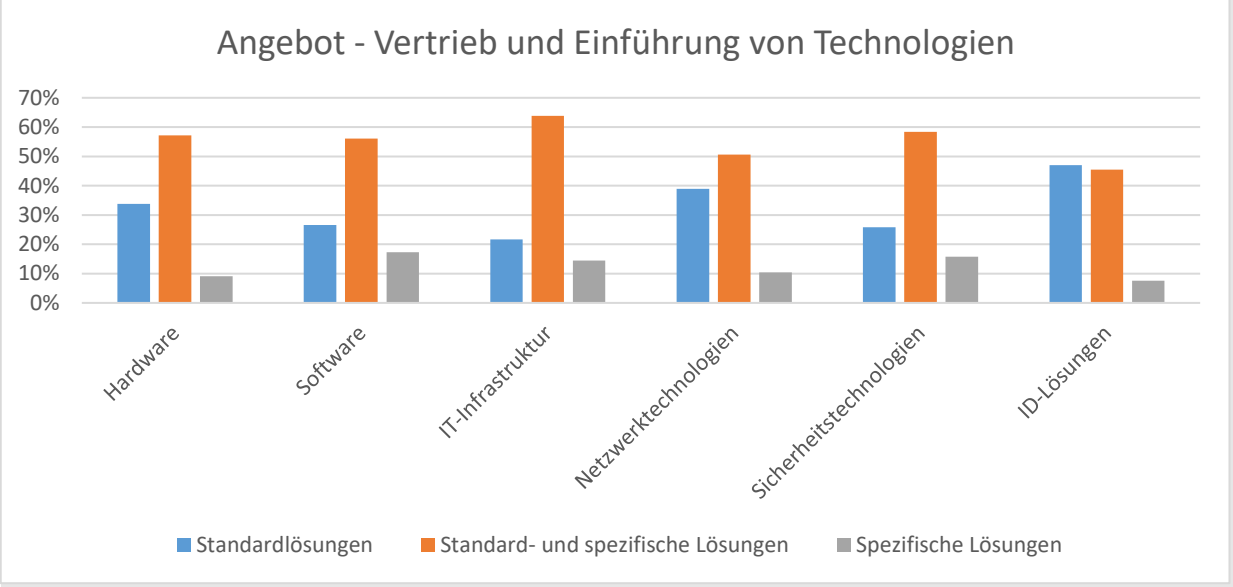

Abbildung 18 – Technologiebereiche in denen IT-Dienstleister verschiedene Lösungen vertreiben.

Bei eigenen Entwicklungen wird, bis auf den Softwarebereich (15%), mehrheitlich auf Standardlösungen gesetzt. Besonders deutlich wird dies bei der Hardwareentwicklung (64%), den ID-Lösungen (57%) und den Netzwerktechnologien (53%).

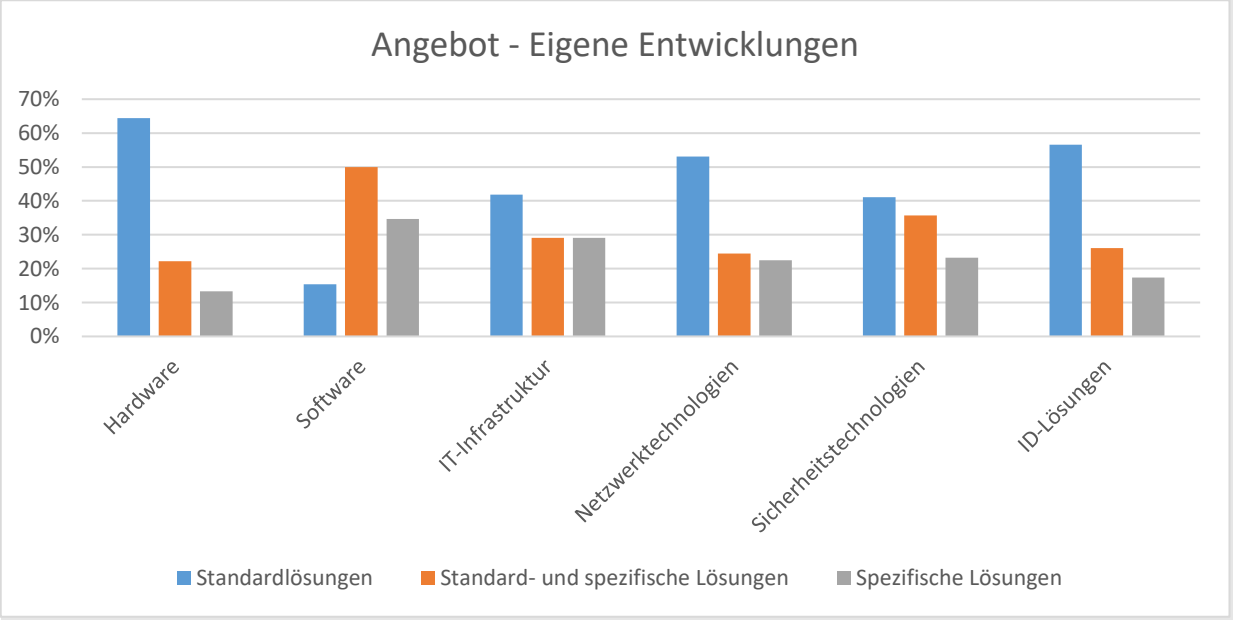

Abbildung 19 – Technologiebereiche in denen IT-Dienstleister verschiedene Lösungen selbst entwickeln.

Bei der Betrachtung der Nachfrageseite zeigt sich ebenfalls, dass mehrheitlich ein Mix aus Standard- und spezifischen Lösungen in fast allen Bereichen angefragt werden. Besonders deutlich ist dies im Bereich Software (63%), IT-Infrastruktur (62%) und Sicherheitstechnologien (56%) der Fall. Rein spezifische Lösungen scheinen kaum nachgefragt zu werden.

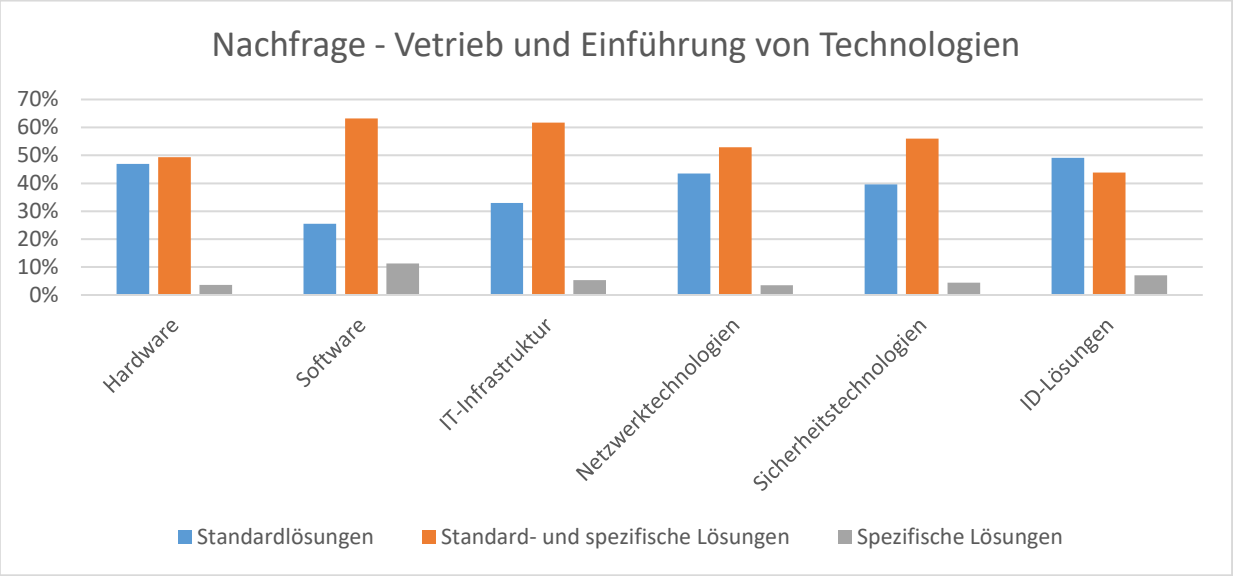

Abbildung 20 – Technologiebereiche in denen IT-Dienstleister verschiedene Lösungen vertreiben.

In der Kategorie der eigenen Entwicklungen zeigt sich jedoch auch, dass im Bereich von Software 30% der Kunden spezifisch für sie geschaffene Lösungen vermehrt nachfragen (siehe Abbildung 21).

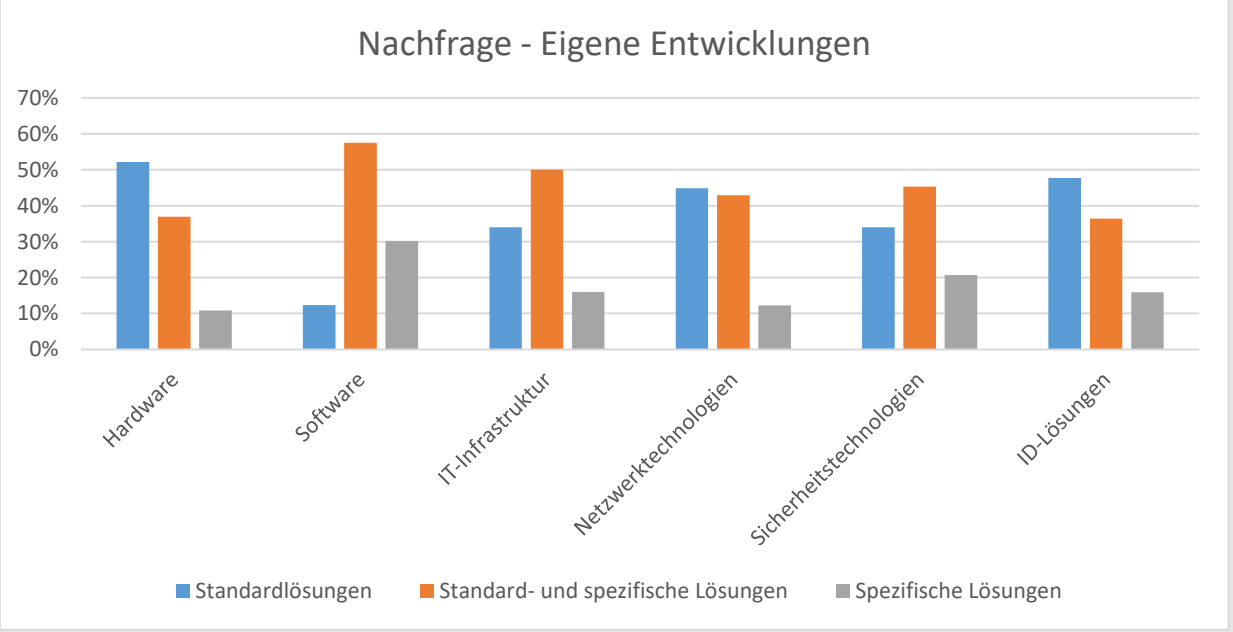

Abbildung 21 – Technologiebereiche in denen IT-Dienstleister verschiedene Lösungen selbst entwickeln.

Darüber hinaus wurden sie gefragt, inwiefern sie Beratung und Services in den folgenden sieben Bereichen anbieten: 1) IT-Dienstleistungen, 2) IT-Beratung, 3) IT-Compliance, 4) Risiko-, Bedrohungs-, und Schutzbedarfsanalyse, 5) IT-Sicherheitskonzepte, 6) Business Continuity Management sowie 7) Checks und Penetrationstest.

Auch hier zeigt sich in allen Bereichen eine klare Tendenz zu hybriden Lösungen. Zwei Drittel und mehr der angebotenen Beratungen oder Services werden als Mix aus standardisierten und spezifischen Lösungen vertrieben. Selbst in den Bereichen Checks und Penetrationstest (53%), Business Continuity Management (59%) sowie IT-Compliance (64%), liegen die Anteile bei z.T. deutlich über der Hälfte. Standardlösungen sind bis auf den Bereich Checks und Penetrationstest, was nicht weiter verwundert, da es sich häufig um wiederkehrende Prüfungsmethoden handelt, in allen Bereichen deutlich unterrepräsentiert.

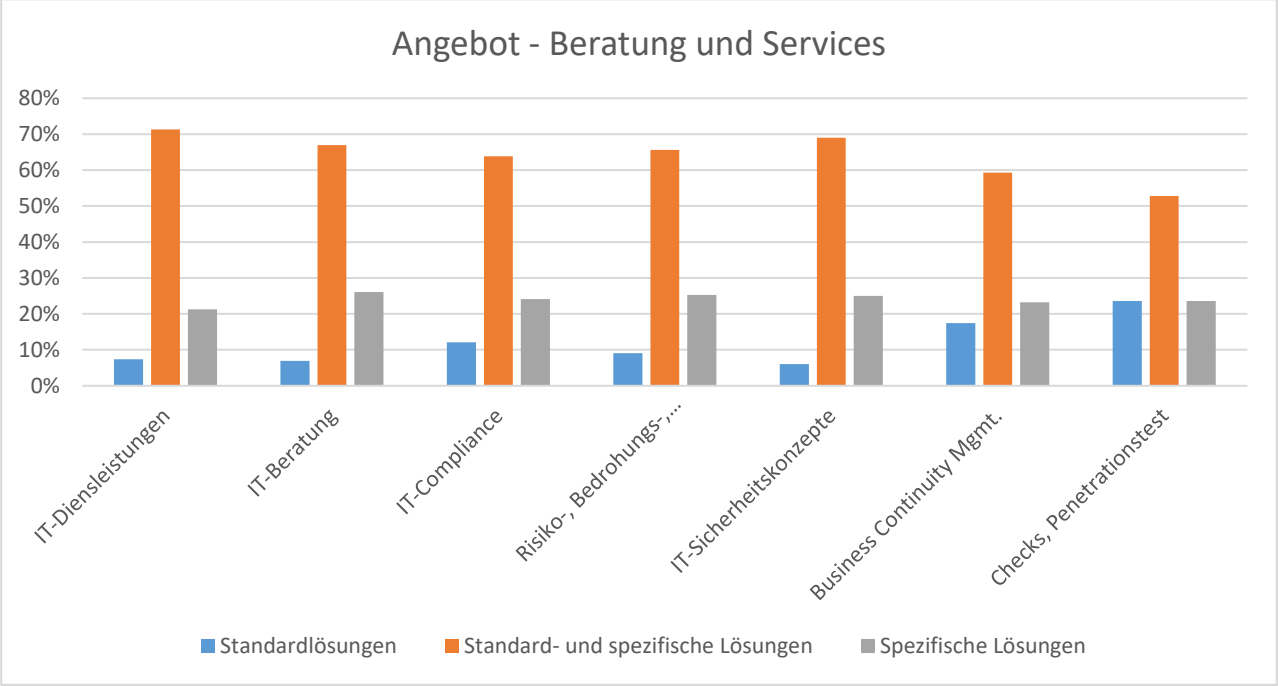

Abbildung 22 – Beratung und Services die IT-Dienstleister in verschiedenen Lösungen anbieten.

Ein fast identisches Bild zeigt sich auf der Nachfrageseite nach Beratungs- und Serviceleistungen. Auch hier werden in allen Bereichen ganz überwiegend hybride Lösungen nachgefragt. Wenig verwunderlich ist, dass insgesamt eine Annäherung der Angebots- und Nachfrageseite stattgefunden hat. Da nach Angaben der IT-Dienstleister vielen ihrer KMU-Kunden ausreichende Kenntnisse im Bereich der Cyber- und IT-Sicherheit fehlen, kann daraus geschlossen werden, dass die IT-Dienstleister die Nachfrage durch ihr Angebot zu einem gewissen Teil steuern. Eine Schlussfolgerung, die im weiteren Verlauf für die Adressierung der Handlungsempfehlungen von Bedeutung ist.

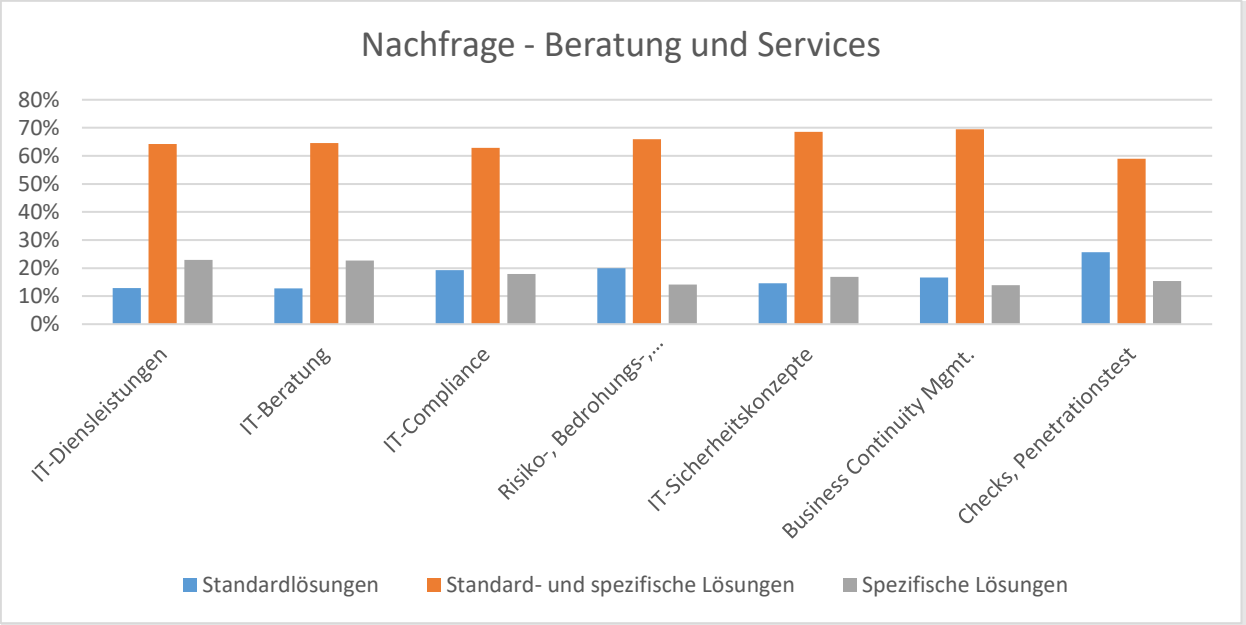

Abbildung 23 – Beratung und Services die als verschiedenen Lösungen nachgefragt werden.

Das Leistungsangebot im Bereich Vorfallmanagement – Analyse, Forensik und Notfallmanagement – zielt ebenfalls eher auf hybride Lösungen ab. Der Bereich Forensik wird fast zu jeweils einem Drittel (Standard 34%, Standard und spezifisch 36%, spezifisch 30%) in allen "Lösungsformen" angeboten.

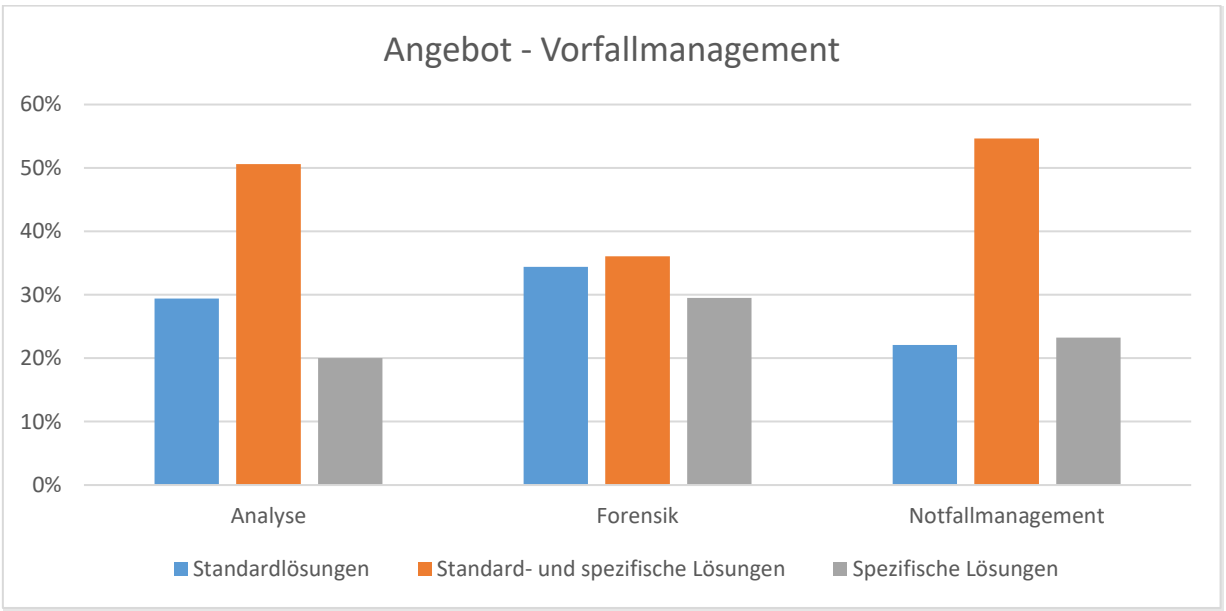

Abbildung 24 – Leistungsangebot im Bereich Vorfallmanagement.

Nachfrage und Angebot sind erneut weitgehend deckungsgleich. Wieder zeigt sich – hier auch im Bereich der Forensik – eine hohe Nachfrage nach einem Lösungsmix aus einem standardisierten und spezifischen Vorfallmanagement.

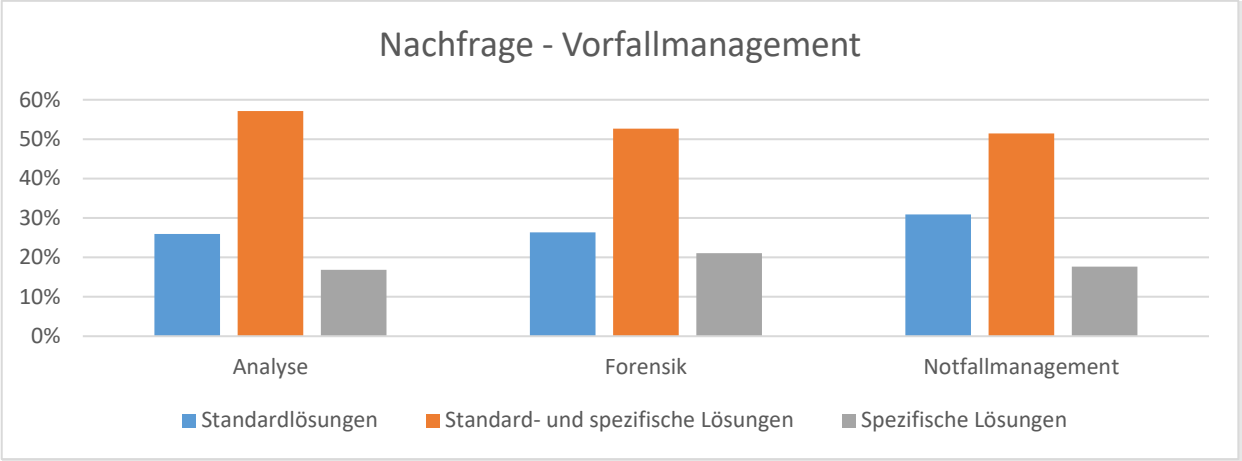

Abbildung 25 – Leistungsnachfragen im Bereich Vorfallmanagement.

Im Bereich der Auditierung und Zertifizierungsberatung werden sowohl mehrheitlich Standardlösungen angeboten als auch nachgefragt. Dies ist keine große Überraschung, da ISO2700X, der BSI Grundschutz und auch andere Zertifizierungen jeweilige Prozess- und Qualitätsstandards verfolgen. Spezifische Lösungen sind nur in Ausnahmefällen relevant, wenn z.B. aufgrund besonderer IT-Sicherheitsinfrastrukturen vorgegebene Standards nicht umgesetzt werden können.

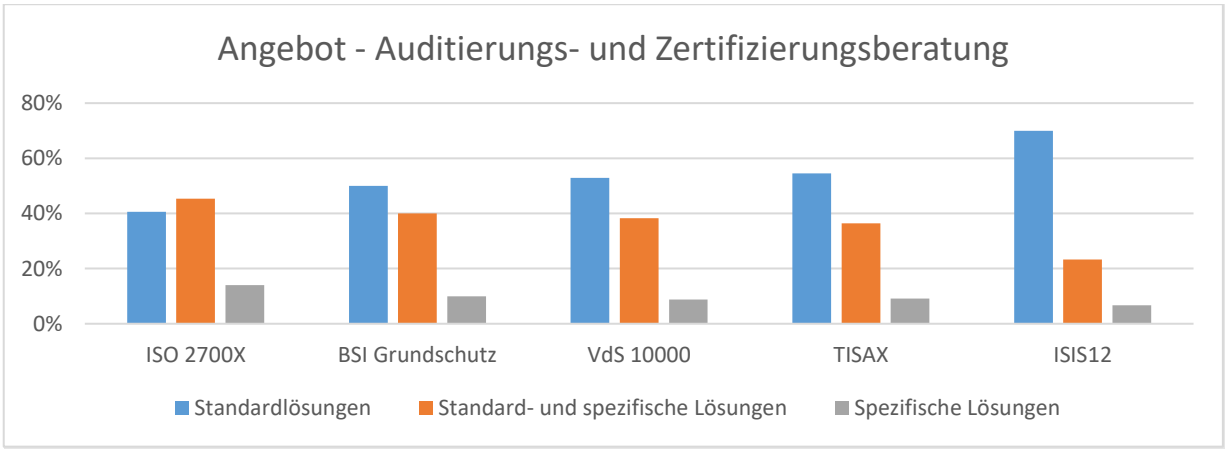

Abbildung 26 – Auditierungs- und Zertifizierungsberatung.

Die ISO 2700X-Reihe von Standards zur Informationssicherheit scheint bei der Nachfrage eine Ausnahme zu bilden. Hier scheint es einen überwiegend hohen Bedarf (56%) an einem Mix aus Standard- und spezifischen Lösungen zu geben.

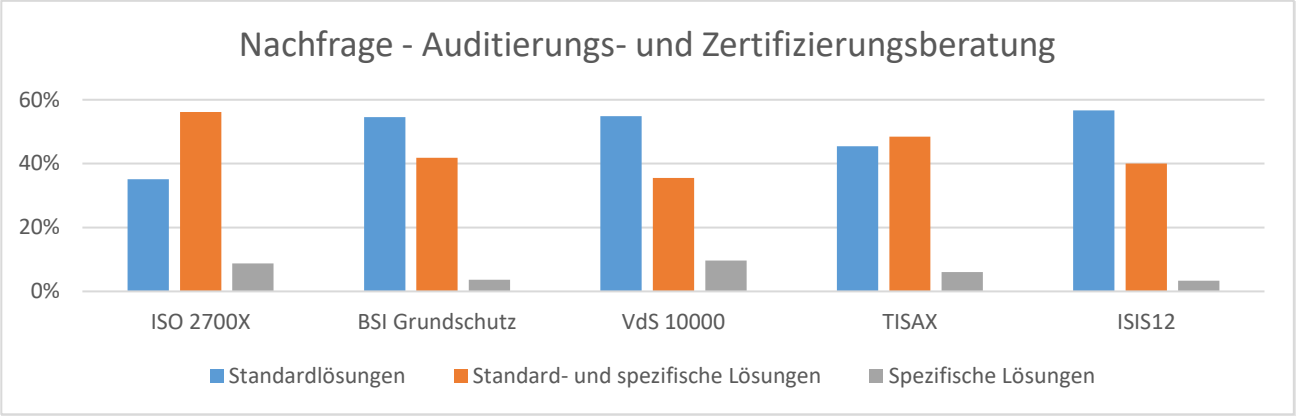

Abbildung 27 – Auditierungs- und Zertifizierungsberatung.

Die Leistungsangebote im Bereich der Schulungen und Awareness sind ebenfalls mehrheitlich auf eine Kombination aus individuellen und standardisierten Lösungen ausgerichtet. Rein standardisierte Schulungen und Programme werden im Vergleich weniger forciert.

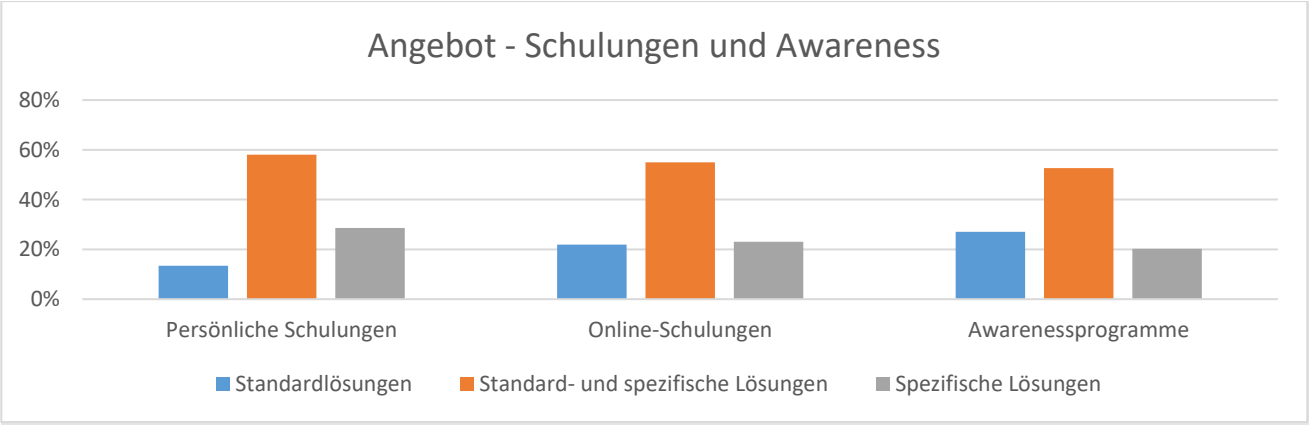

Abbildung 28 – Schulungen und Awarenessprogramme.

Schließlich wurden die IT-Dienstleister auch nach Angeboten in anderen, nicht abgefragten Bereichen gefragt. Bei insgesamt 69 Antworten stach insbesondere der Bereich Datenschutz hervor. Insgesamt 11 Antworten zählten unterschiedliche Dienstleistungen in diesem Bereich auf (z.B. Beratung zu Schulungen, Fragen zur Stellung des Datenschutzbeauftragten). Ein weiterer, häufig genannter Bereich umfasst IT-Sicherheit (8x) sowie den Bereich Managed Services (5x). Die Antworten zeigen ein sehr vielfältiges Angebotsspektrum, von der Automatisierungsberatung, über die Beratung des kompletten Lebenszyklus im Bereich Software, bis hin zu Social Media und Rechercheunterstützung.

Bei der Betrachtung des Produktportfolios sollte vor dem Hintergrund der angewandten Methodik beachtet werden, dass die IT-Dienstleister ihre Fähigkeiten tendenziell eher über- als unterbewerten werden.

7.2.4. Qualifikation und Weiterbildung der MitarbeiterInnen

Eine besondere Bedeutung kommt der spezifisch-technischen Berufsausbildung (FachinformatikerIn, EntwicklerIn, etc.) bei der Auswahl und der Einstellung von Mitarbeitern bei IT-Dienstleistern zu. Für fast die Hälfte der IT-Dienstleister (49%) ist diese Qualifikation mit Abstand *eher wichtig* und für 17% *sehr wichtig*. Diese Antworten verdeutlichen, dass PraktikerInnen sehr gefragt sind und ein abgeschlossenes Hochschulstudium nicht unbedingt ein Einstellungskriterium in dieser Branche darstellt (Credo: „Wir brauchen Leute, die machen und weniger welche, die drüber nachdenken!“).

Damit ist fast jeder vierte von fünf IT-Dienstleister der Meinung, dass eine spezifisch-technische IT-Berufsausbildung von besonderer Relevanz bei der Auswahl geeigneter MitarbeiterInnen ist. Im Vergleich zu anderen Auswahl- und Einstellungskriterien ist dies der mit Abstand höchste Wert. Fast die Hälfte (46%) der IT-Dienstleister (33% *eher wichtig*, 13% *sehr wichtig*) sind zudem der Meinung, dass ein einschlägiges Studium im Bereich der Informatik/ IT-Sicherheit ein wichtiges Auswahlkriterium darstellt. Etwa ein Drittel (25% *eher wichtig*, 5% *sehr wichtig*) sehen diese Relevanz beim dualen Studium, wobei es ein fast gleich großer Anteil (4% *sehr unwichtig*, 23% *eher unwichtig*) als für nicht allzu relevant ansieht.

Ein allgemeines technisches Studium (z.B. Ingenieurwesen) scheint keine herausragende Rolle zu spielen. Auch QuereinsteigerInnen werden nur bedingt gesucht. Dies hängt selbstverständlich mit der Situation am Arbeitsmarkt – Stichwort Fachkräftemangel – zusammen und von Faktoren wie Unternehmensgröße, Strahlkraft, Budget, Region, etc. ab. Es ist davon auszugehen, dass mit der Zunahme des Fachkräftemangels auch die Möglichkeiten für QuereinsteigerInnen sich erhöhen.

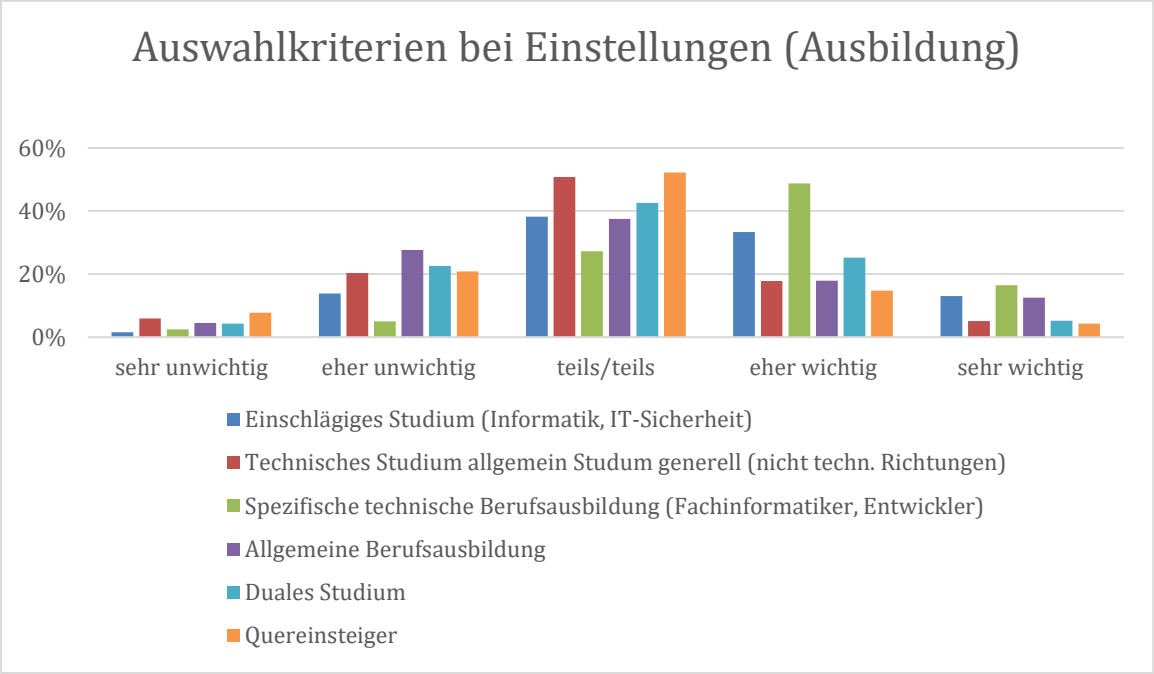

Abbildung 29 – Auswahlkriterien bei der Einstellung geeigneter MitarbeiterInnen für den IT- und IT-Sicherheitsbereich.[144]

Im Weiterbildungskontext spielen für IT-Dienstleister drei Aspekte eine größere Rolle: Kenntnisse durch Weiterbildung im Umgang mit der ISO 2700x Reihe fanden 34% für *eher wichtig* und 13% für *sehr wichtig*. Weitere 30% bewerten sie mit *teils/teils*. Kenntnisse des BSI Grundschutz fanden 33% für *eher wichtig*, bzw. 10% für *sehr wichtig*, sowie 36% für *teils/teils*. Zertifizierungen im Rahmen von Partnerprogrammen wie z.B. große Hard- und Softwareanbieter erachten 33% als ein *eher wichtiges* und 19% als ein *sehr wichtiges* Auswahlkriterium. Fast ein Drittel (28%) bewerten es „neutral". Dies ist insbesondere darauf zurückzuführen, dass der Partnerstatus eines Unternehmens bei den großen Systemanbietern wesentlich von der Anzahl der zertifizierten MitarbeiterInnen abhängt. Ein hoher Partnerstatus erhöht die Sichtbarkeit, und sichert bessere Einkaufskonditionen.

Fest steht, und das ist ebenfalls keine große Überraschung, dass BewerberInnen mit Zusatzqualifikationen einen Vorteil beim Bewerbungsverfahren haben. Dies hängt jedoch von der Arbeitsmarktsituation ab.

[144] Frage: Nun interessiert uns, welche Aspekte Ihnen als IT-Dienstleister bei der Auswahl und der Einstellung geeigneter MitarbeiterInnen für den IT- und IT-Sicherheitsbereich besonders wichtig sind. Bitte kreuzen Sie an, wie wichtig Ihnen die einzelnen Punkte sind.

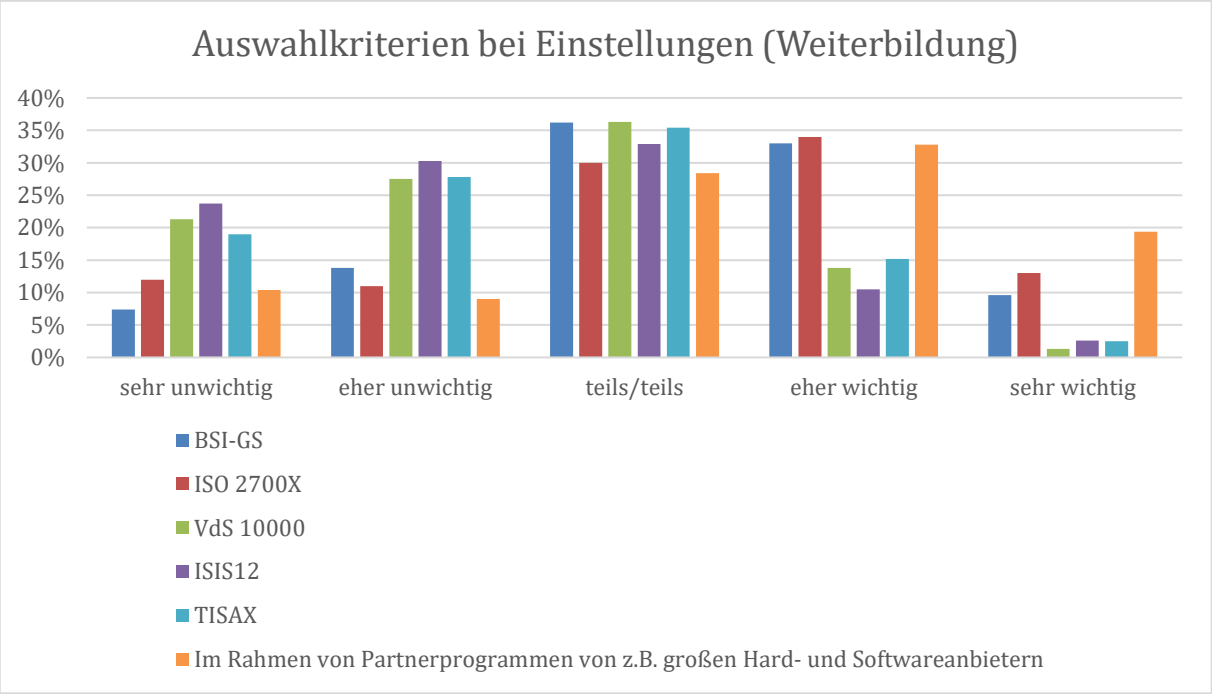

Abbildung 30 – Auswahlkriterien bei der Einstellung geeigneter MitarbeiterInnen für den IT- und IT-Sicherheitsbereich.

In diesem Zusammenhang wird unterstrichen, dass IT-Dienstleister einen *eher wichtigen* bis *sehr wichtigen* Zusammenhang zwischen der Aus- und Weiterbildung ihrer MitarbeiterInnen und ihrem Erfolg im KMU-Kundensegment sehen (insgesamt 79%). Der Unternehmenserfolg ist somit stark an die Qualifikationen der MitarbeiterInnen gekoppelt und schafft eine gewisse Abhängigkeit. Dass gute Qualifikationen eine übergeordnete Rolle für den Erfolg eines Unternehmens spielen, dürfte nicht weiter verwundern. QuereinsteigerInnen werden Wertschätzung häufiger dort erfahren, wo Führungskräfte ohne passende Ausbildung selbst ähnliche Erfahrungen gemacht haben. Der Konkurrenzkampf um Fachkräfte beeinflusst sowohl die Expansionsmöglichkeiten als auch die Produktqualität.

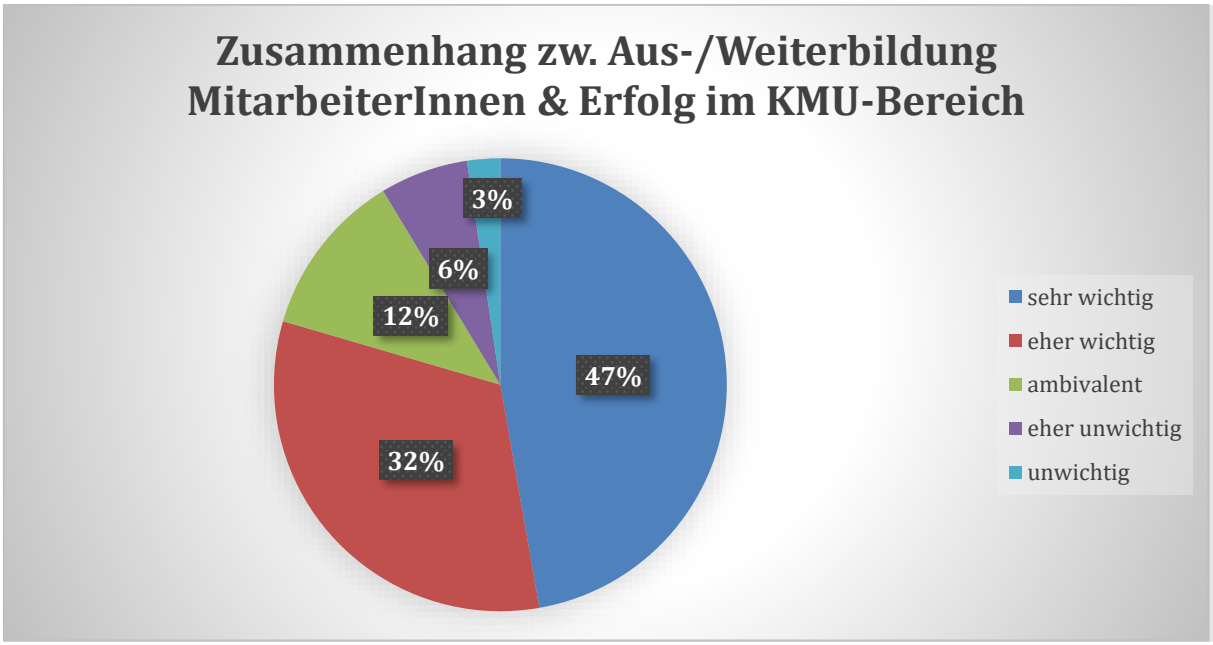

Abbildung 31 – Bewertung der Bedeutung des Zusammenhangs von Ausbildung/ Weiterbildung/ Zertifizierung der MitarbeiterInnen im Unternehmen und Erfolg des Unternehmens im KMU-Kundensegment.

In diesem Zusammenhang ist auch die Frage nach der Relevanz individueller Expertisen (der MitarbeiterInnen) für die IT-Dienstleister bei der Beratung von KMU interessant. Dabei stellen sich vier Aspekte als *sehr wichtig* heraus: 1. Prozess- und Methodenwissen (54%); 2. Aktuelle Sicherheitsinformationen (45%); 3. IT-Sicherheitskräfte/MA (38%) sowie 4. Branchenwissen (33%). Somit spielen für die IT-Dienstleister sowohl die Qualifikationen/Ausbildung (ihrer MitarbeiterInnen) eine herausragende Rolle (Punkt 1. und 3.) bei der Kundenbetreuung, als auch fundierte Kenntnisse der MitarbeiterInnen in den Branchen der KMU-Kunden, die darüber hinaus Willens sind, sich weiterzubilden, um stetig über aktuelle Sicherheitsbedrohungen informiert zu sein.

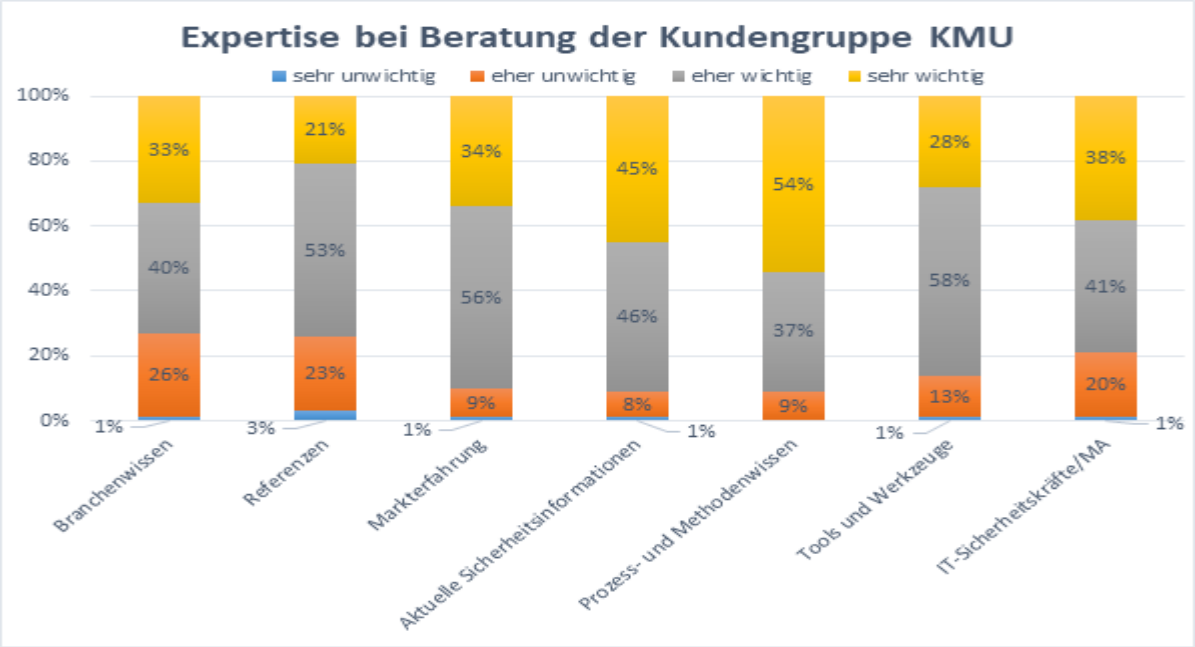

Abbildung 32 – Relevanz der Expertise bei der Beratung von KMU.

Bei der Betrachtung der relevantesten Faktoren im KMU Kundensegment wird allerdings auch deutlich, dass die Servicequalität (65%) und die Wirtschaftlichkeit (56%) für die IT-Dienstleister eine besondere Rolle spielen. Hier liegt der Fokus scheinbar auf Nachhaltigkeit in Bezug auf die Servicequalität, was selbstverständlich auch mit der Qualifikation der MitarbeiterInnen zusammenhängt (35%), und darauf mit den gegebenen Mitteln den größtmöglichen Ertrag zu erwirtschaften.

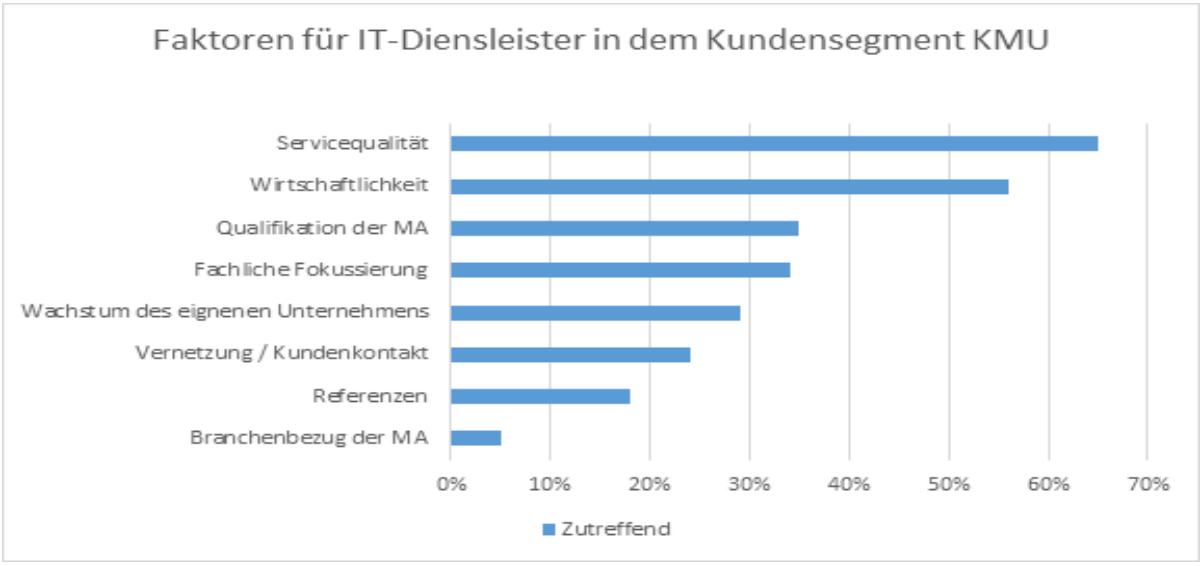

Abbildung 33 – Relevante Faktoren für IT-Dienstleister in dem Kundensegment KMU.[145]

[145] Frage: Welche Faktoren spielen für Sie als IT-Dienstleister in dem Kundensegment KMU eine besondere Rolle? (max. 3 Angaben möglich).

7.2.5. Marketingkommunikation/ Neukundenakquisition

Empfehlungen scheinen bei der Neukundenakquisition für IT-Dienstleiser im KMU-Kundensegment eine gewichtige Rolle zu spielen. 56% der Befragten gaben an, dass Empfehlungen *sehr häufig* und 33% *eher häufig* entscheidend für die Neukundenakquisition sind. Das ist der mit Abstand höchste Wert.

Darüber hinaus ist die Imagepflege über z.B. Partnerschaften und Konferenzen bei 27% ein *sehr häufig* und bei 33% ein *eher häufig* eingesetztes Instrument zur Neukundengewinnung.

Auch über Verbände und Netzwerke als Vermittler bzw. Ansprechpartner für KMU (16% *sehr häufig*, 28% *eher häufig* und 32% *gelegentlich*) scheint ein signifikanter Anteil an Neukunden gewonnen zu werden.

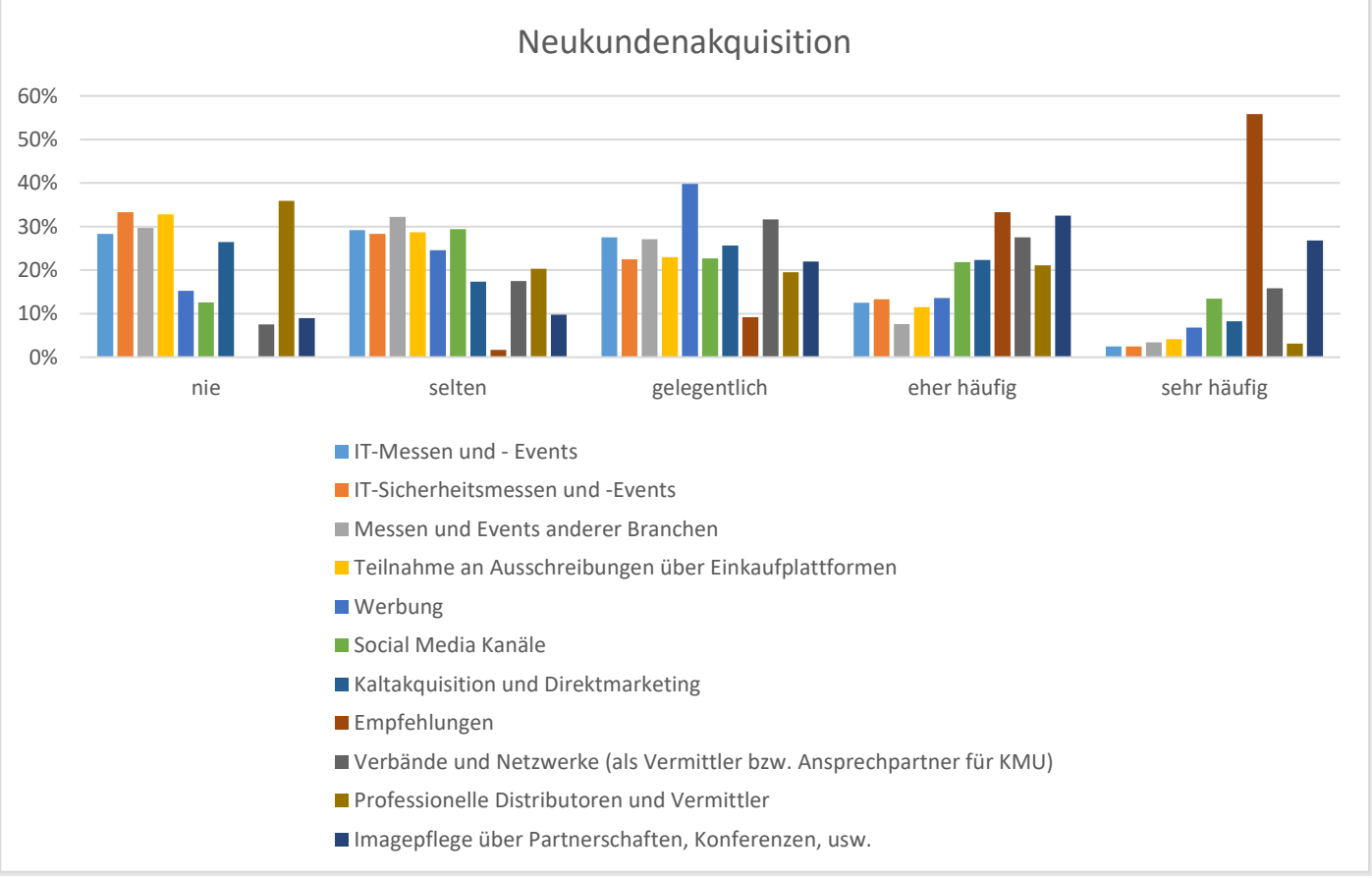

Abbildung 34 – Wege der Neukundenakquisition der IT-Dienstleister in der Kundengruppe der KMU.[146]

[146] Frage: Wir betrachten nun Ihre Neukundenakquisition in der Kundengruppe der KMU. Bitte kreuzen Sie an, wie häufig Sie die angegebenen Wege nutzen, um neue Kunden zu gewinnen!

Insgesamt gaben 45% der IT-Dienstleister an, dass ihnen die Neukundenakquisition im KMU-Segment mit der Kategorie „klein“ (10-49 MitarbeiterInnen) *eher leicht* bzw. *leicht* fällt, während 20% es als *eher schwer* bzw. *schwer* empfinden; 32% *teils/teils*. Während 35% der Befragten die Neukundenakquisition in der kleinsten KMU Kategorie (bis 9 MitarbeiterInnen) als *eher leicht* oder *leicht* ansehen, haben ein Fünftel (21%) der IT-Dienstleister gar kein Interesse an Kunden in dieser Größenkategorie. Eine Vermutung wäre, dass aufgrund schwieriger Planbarkeit bzw. Wirtschaftlichkeit einige IT-Dienstleister solche Kundengrößen meiden. Darüber hinaus könnten Ressourcen (Humankapital) knapp sein und somit dort eingesetzt werden, wo sie den größten Mehrwert für den Arbeitgeber liefern.

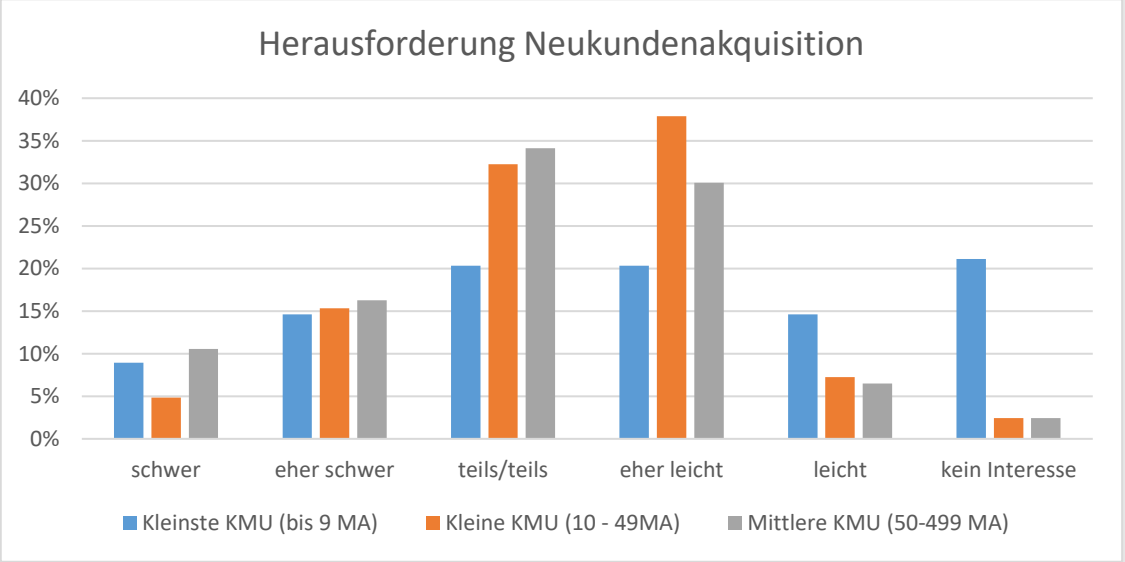

Abbildung 35 – Neukundenakquisition nach KMU Größe und Schwierigkeitsgrad.

Der Erstkontakt in der Kategorie „kleinste“ und „kleine“ KMU läuft in der deutlichen Mehrheit über die Geschäftsführung (91% bis 9 MA; 75% 10-49 MA). In KMU der Kategorie „mittel“ läuft der Erstkontakt in aller Regel über die IT-Abteilung (58%). Eine solche Abteilung ist bei vielen kleinsten und kleinen KMU nicht vorhanden sein. Dort werden fast alle relevanten Entscheidungen vom Eigentümer bzw. der Geschäftsführung getroffen und erklären die nicht überraschend unterschiedlichen Herangehensweisen.

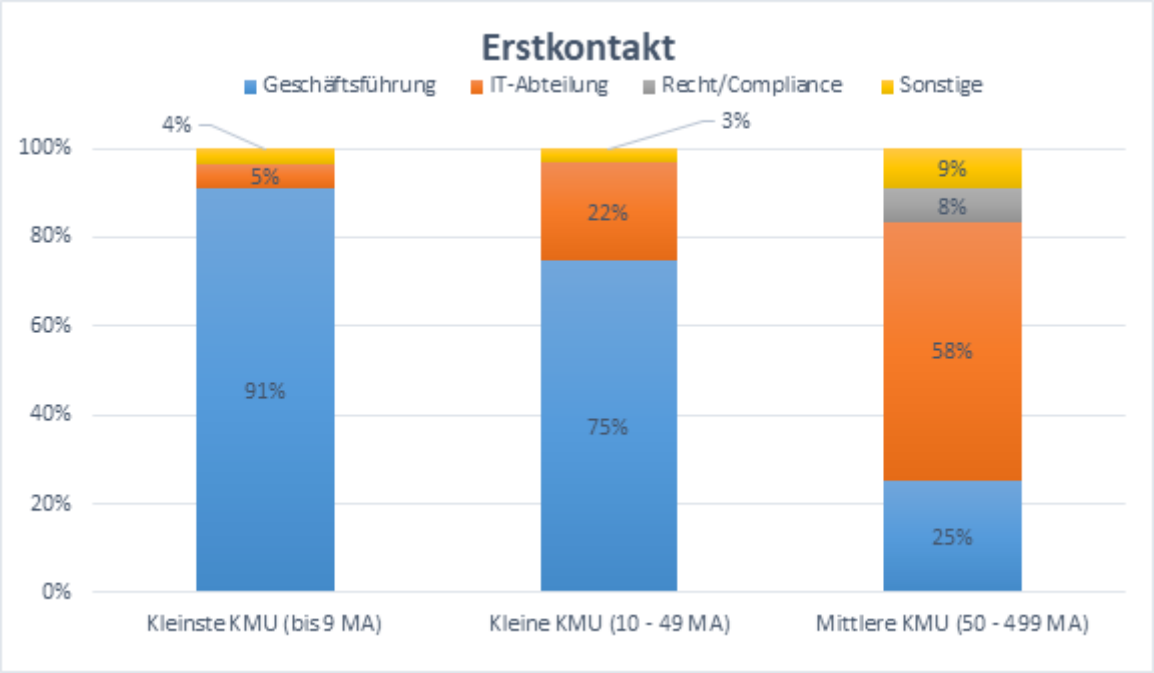

Abbildung 36 – Ansprechpartner bei Erstkontakt mit KMU.

Die Geschäftsführung bleibt auch in der weiteren Zusammenarbeit eine wichtige Anlaufstelle. Für fast die Hälfte (48%) der IT-Dienstleister ist die Geschäftsführung *häufig*, für 31% sogar *immer* der Ansprechpartner. Zudem arbeiten 44% der IT-Dienstleister *häufig* und 41% *immer* mit festen AnsprechpartnerInnen/ProjektmanagerInnen zusammen. Die Zusammenarbeit mit KMU als Kunden läuft laut der befragten IT-Dienstleister nur in 19% *immer*, in 45% *häufig* und in 26% der Fälle *gelegentlich* über die fachliche Ebene. Dies zeigt, wie wichtig es ist, mit den späteren Handlungsempfehlungen die Leitungsebene der KMU zu adressieren.

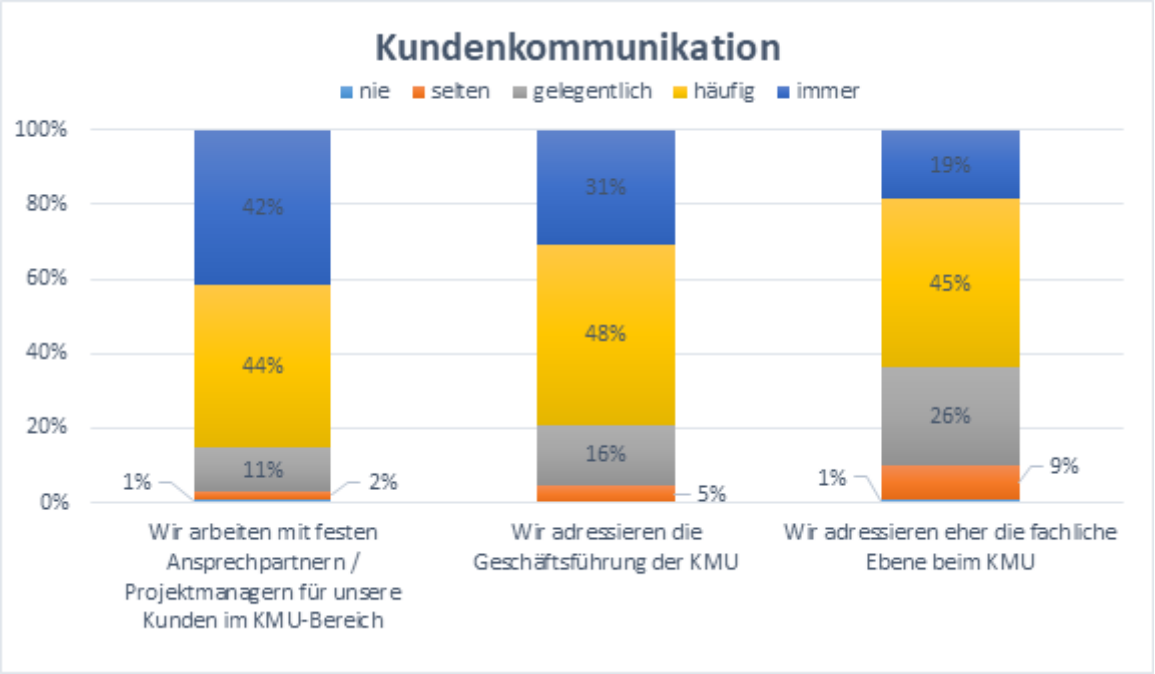

Abbildung 37 – Kommunikationswege bei der Zusammenarbeit mit KMU.[147]

9 von 10 IT-Dienstleister gaben an, dass sie im KMU-Kundensegment gerne weiterwachsen würden. Die IT-Dienstleister, die dies nicht forcieren, gaben dafür vor allem eine geringere Wirtschaftlichkeit der Aufträge (24%), eine geringere Marktattraktivität im KMU-Bereich (18%) sowie eine schwierige Planbarkeit der Projekte bzw. Aufträge an (18%). Die Ursachen dafür könnten u.a. in der oftmals unklaren Entscheidungsstruktur, dem kleinteiligen Auftragsvolumen, der fehlenden Sensibilisierung bei EntscheidungsträgerInnen und der damit einhergehenden fehlenden Allokation eines entsprechenden Budgets sowie des ungleich höheren Aufwands für individuelle Leistungen, die sich selten skalieren lassen und somit höhere Kosten verursachen, liegen.

7.2.6. Kooperationsplattformen und Netzwerke

Eine entscheidende Frage aufgrund großer Lücken in der bisherigen Datenlage war auch, wie IT-Dienstleister miteinander vernetzt sind bzw. sich über aktuelle Sicherheitsthemen informieren. *Existieren Multiplikatoren im Bereich der IT-Dienstleister für KMU? Sind IT-Dienstleister in Verbänden oder Netzwerken organisiert?*

Die Ergebnisse der Umfrage zeigen, dass IT-Dienstleister mehrheitlich mit anderen IT-Sicherheitsdienstleistern kooperieren. Dies erfolgt entweder aus eigenem Antrieb heraus oder auf Wunsch des Kunden. Darüber hinaus sind IT-Dienstleister im engen Kontakt mit der IHK (49%), mit Verbänden (39%) sowie anderen Netzwerken (42%). Insbesondere mit

[147] Frage: Nachfolgend sehen Sie einige Beschreibungen, wie die Zusammenarbeit mit KMU als Kunden für IT-Sicherheit grundsätzlich aufgebaut sein kann. Bitte kreuzen Sie das auf Ihr Unternehmen am ehesten zutreffende an!

BITKOM e.V. (21%), iTeam Systemhauskooperation (15%), der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) (11%) sowie dem Bundesverband mittelständische Wirtschaft (BVMW) (10%) sind die befragten IT-Dienstleister im engeren Kontakt zur Kooperation sowie zum themenspezifischen Informationsaustausch. Vor dem Hintergrund der "sozialen Erwünschtheit" sollte auch hier erwähnt werden, dass viele dieser Netzwerke und Plattformen ebenfalls als Multiplikatoren für die Bekanntmachung der Befragungslinks und für die Suche nach Interviewpartner genutzt wurden.[148]

Auf der Netzwerkseite sind hier insbesondere eigene Firmen- und Partnernetzwerke von Relevanz sowie soziale Netzwerke wie LinkedIn, Facebook, XING u.a. (9%). Insgesamt wurden 49 verschiedenen Verbände bei 52 Antworten bei der Frage nach engerem Kontakt für Kooperation und Austausch genannt. Auf der Netzwerkseite wurden 48 verschiedene Netzwerke bei insgesamt 55 Antworten genannt. Dabei gab es jedoch eine Überschneidung zwischen den genannten Verbänden aus dem zweiten Teil der Frage und den genannten Netzwerken.

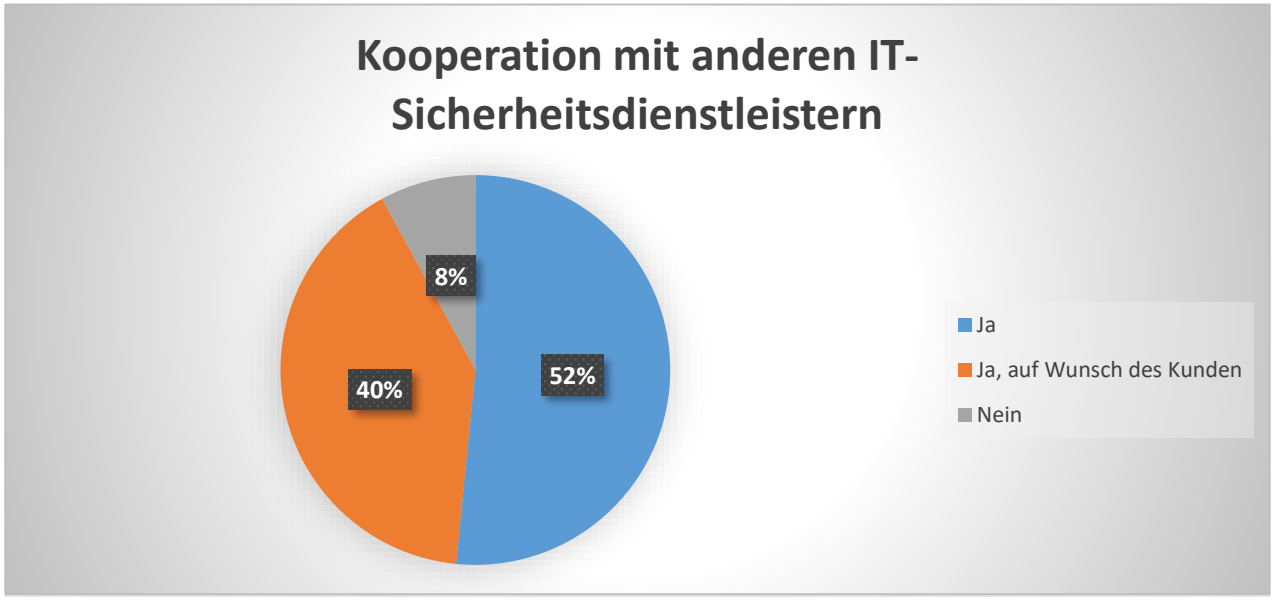

Abbildung 38 – Kooperationsbereitschaft mit anderen IT-Dienstleistern.

Insgesamt 62 Befragte gaben an, dass ihr Unternehmen in einem Verband Mitglied ist. Dabei wurden 62 unterschiedliche Verbände in 127 Antworten genannt. Am häufigsten sind die IT-Dienstleister Mitglied im Bundesverband mittelständische Wirtschaft (11x). Des Weiteren BITKOM (9x), die iTeam Systemhauskooperation (7x) und die Gesellschaft für Datenschutz und Datensicherheit e.V. sowie die Allianz für Cybersicherheit, welche jeweils 6x genannt wurden.

[148] Den Einfluss auf die Ergebnisse halten wir dennoch für eher gering.

Die Verbände werden zudem als Informationsquellen genutzt, wobei Netzwerke (99x) die wichtigste Informationsquelle für aktuelle IT-Sicherheitsprobleme für die IT-Dienstleister sind. Danach folgt der BSI-Lagebericht (85x) sowie (andere) IT-Sicherheitsfirmen (83x) und die Allianz für Cyber-Sicherheit (66x).[149]

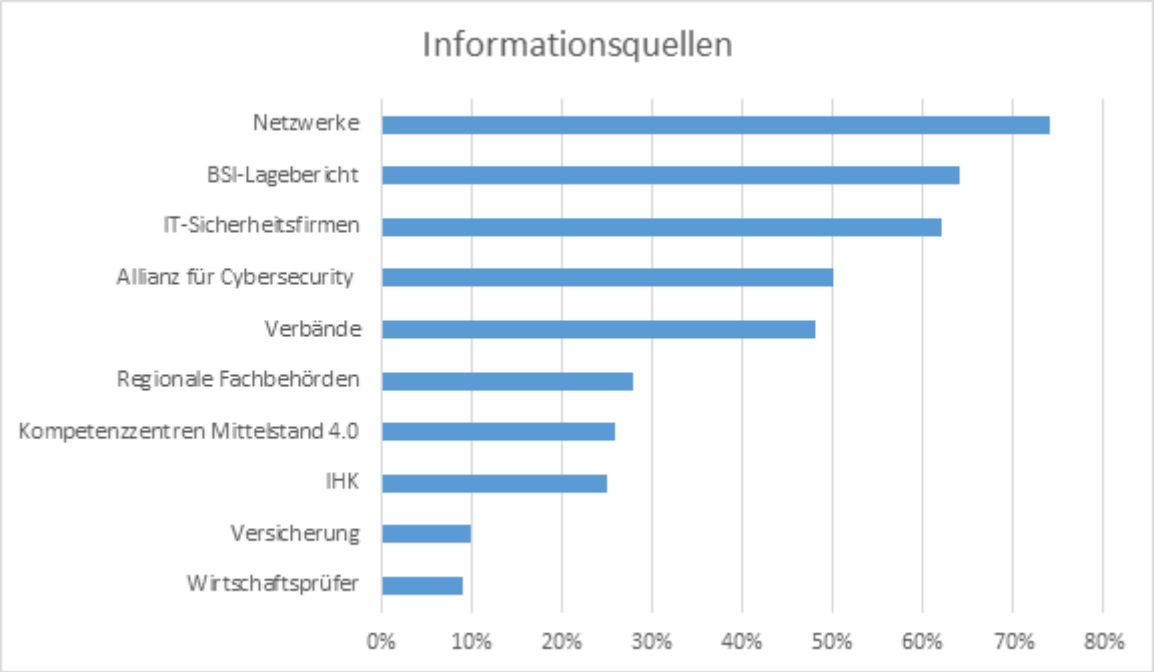

Abbildung 39 – Die fünf wichtigsten Informationsquellen für IT-Dienstleister.

7.2.7. Öffentliche Förderung

Die Wirksamkeit öffentlicher Fördermaßnahmen im Bereich der IT- und Cybersicherheit für KMU hängt auch mit dem Bekanntheitsgrad und den Rahmenbedingungen zusammen. Sind Förderprogramme unbekannt oder die Beantragung aus Sicht der KMU zu umständlich, verfehlen sie schon allein deswegen ihre wirtschaftspolitische Wirkung. Vor diesem Hintergrund sind Einsichten und Interna, die die IT-Dienstleister bei und von ihren KMU-Kunden haben, für mögliche Optimierungsansätze öffentlicher Fördermaßnahmen besonders relevant. Ebenso unerlässlich ist die Informationspolitik mit und zu den IT-Dienstleistern. Die Bekanntheit verschiedener Fördermaßnahmen und die damit verbundenen Chancen und Ansätze innerhalb dieser Netzwerke, kann eine erhebliche Sichtbarkeit schaffen, da IT-Dienstleister solche Informationen über ihre Netzwerke in die KMU hineintragen können.

Insgesamt wurden 60 verschiedene Programme bei 230 gewerteten Antworten genannt. Bei dem mit großem Abstand am häufigsten genannte Förderprogramm handelt es sich um „go-digital“ vom BMWi (86x). Danach folgen die Digital-

[149] Frage: Welche Informationsquellen sind für Sie besonders wichtig? Bitte ordnen Sie die wichtigsten fünf per *drag and drop* ein! n=133.

boni der verschiedenen Bundesländer (13) sowie das Förderprogramm mit dem Namen „Förderung unternehmerischen Know-hows“ des BMWi (10x). 16 der Befragten gaben an, dass sie keine öffentlichen Fördermaßnahmen kennen.

In einer Folgefrage bzgl. wünschenswerter Fördermaßnahmen aus Sicht der IT-Dienstleister für den IT-Bereich fallen zwei Forderungen auf: 1. Die gezielte Förderung von IT-Sicherheit (11x) und in diesem Zusammenhang auch die gezielte Förderung von IT-Sicherheitsdienstleistungen (5x); 2. Weiterbildung und Aufklärung über Risiken bei MitarbeiterInnen sowie der Geschäftsführung (12x). Darüber hinaus wünschen sich einige der Befragten (6x) eine modifizierte Förderung von „go-digital“, z. B. durch die Ausweitung dieser auf Ärzte und/oder Freiberufler, die besonders sensible personenbezogene Daten verarbeiten.

Darüber hinaus gab es 17 Anmerkungen/Kommentare bei 22 gewerteten Antworten zu den Rahmenbedingungen von Fördermaßnahmen: So sollte sich beispielsweise der Aufwand für die Beantragung für Fördermaßnahmen vereinfachen (4x) und diese sollten schneller bearbeitet werden (2x). So schrieb einer/e der Befragten, dass der Antrag „unkompliziert und ohne ewige Beraterkonzepte und lange Antragstellung“ erfolgen sollte und ein/e weitere/r, dass es an „sich genug Förderprogramme [gibt]. Das Problem ist, das Richtige zu finden und dann noch richtig zu beantragen.“

7.2.8. Besondere Hemmnisse

Als besondere Hemmnisse, denen IT-Dienstleistern im KMU-Segment begegnen, stechen drei signifikante heraus:

1. Fehlendes Budget (31x bei 130 gewerteten Antworten): Aus Sicht der IT-Dienstleister ist es den KMU entweder nicht möglich oder sie sehen nicht den Mehrwert des zu investierenden Budgets für IT-Sicherheit bzw. generell für eine sichere IT-Infrastruktur. Dieses Hemmnis ist wenig überraschend, da Budgetrestriktionen in KMU eher die Regel als die Ausnahme sind, vor allem in Bereichen, in denen der Mehrwert für Entscheidungsträgern nicht komplett nachvollziehbar ist. Ein fehlendes Grundverständnis, die IT-Sicherheit als Unternehmensressource und nicht als entbehrlichen Kostenfaktor zu betrachten, ist häufig die Ursache.
2. Dies steht vermutlich auch mit der fehlenden Sensibilität (27x) für das Thema im Zusammenhang: Die IT-Dienstleister bescheinigen vielen KMU zu wenig Sensibilität für IT-Sicherheit und damit zusammenhängend auch zu wenig strategische Weitsicht, um die richtigen Investitionsentscheidungen zu treffen. Einige KMU scheinen IT-Sicherheit immer noch als etwas zu betrachten, dass sie nicht betrifft oder mit dem sie sich nicht beschäftigen müssen (Credo: „Wir sind zu klein, uns betrifft das nicht“).
3. Wissen/Grundverständnis für IT sowie IT-Sicherheit (23x): IT-Dienstleister bemängeln ein unzureichendes Know-how bzw. fehlendes Grundverständnis für den Themenbereich. Dieser Punkt wird immer wieder bei verschiedenen Fragen von IT-Dienstleistern aufgeführt.

Weitere häufige genannte Hemmnisse sind eine fehlende Investitionsbereitschaft, möglicherweise aufgrund der drei oben genannten Aspekte (7x). Hinzukommen Management- und Organisationsprobleme in den KMU (9x). Aber auch ein Mangel an qualifizierten MitarbeiterInnen in den KMU (4x) sowie Angst bzw. Skepsis vor dem Themenbereich IT (4x) werden mehrfach genannt. Des Weiteren werden einige erst nach einem Schadensfall aktiv (4x) („Aus Schaden wird man klug“).

Der Budgetaspekt und ein eventuell damit zusammenhängendes fehlendes Grundverständnis spiegelt sich auch in der Frage nach der Unterscheidung zwischen IT- und IT-Sicherheitsbudgets wider, sowie ob KMU-Kunden über speziell ermittelte bzw. ausgewiesene IT-Sicherheitsbudgets in der Planung verfügen.

Der Umgang mit und das Verständnis für das Thema IT- und IT-Sicherheit zeigt sich auch in einer weiteren Frage. 27% der IT-Dienstleister gaben an, dass ihre KMU-Kunden bei der Planung nicht zwischen IT- und IT-Sicherheitsbudgets unterscheiden. Weitere 39%, dass dies nur bei wenigen KMU-Kunden der Fall sei. Lediglich 3% gaben an, dass eine Unterscheidung bei allen Kunden vorgenommen wird. Darüber hinaus führen 34% an, dass *keiner* ihrer KMU-Kunden über ein speziell ausgewiesenes IT-Sicherheitsbudget verfügt und weitere 40%, dass dies bei *fast kein*em KMU-Kunden der Fall sei.

Dass die Sensibilisierung für Risiken und Gefahren im IT-Bereich weiterhin ein wichtiges Thema für eine Verbesserung des IT-Sicherheitsniveaus ist, zeigt sich auch in der Umfrage. Auf die Frage „*Welche der folgenden Aspekte gesellschaftlich dringend geändert werden müssten, um die Zusammenarbeit mit KMU zu erleichtern und damit die IT-Sicherheit in Deutschland zu verbessern?*“[150] zählten „Sensibilisierung für Risiken und Gefahren im IT-Bereich“ mit 54% sowie „(Schulische) Bildung im Bereich Digitalisierung stärken“ mit 47%, zu den mit Abstand am häufigsten genannten Antworten. Zu den weiteren Nennungen gehörten auch die Vereinfachung von öffentlicher Förderung (35%) und in diesem Zusammenhang auch das Herunterbrechen von Anforderungen und Bürokratieabbau in diesem Bereich (32%). Awareness bei KMU für IT-Sicherheit ist ein immer wieder gern aufgeführter Punkt (29%).

[150] Es waren maximal drei Nennungen möglich.

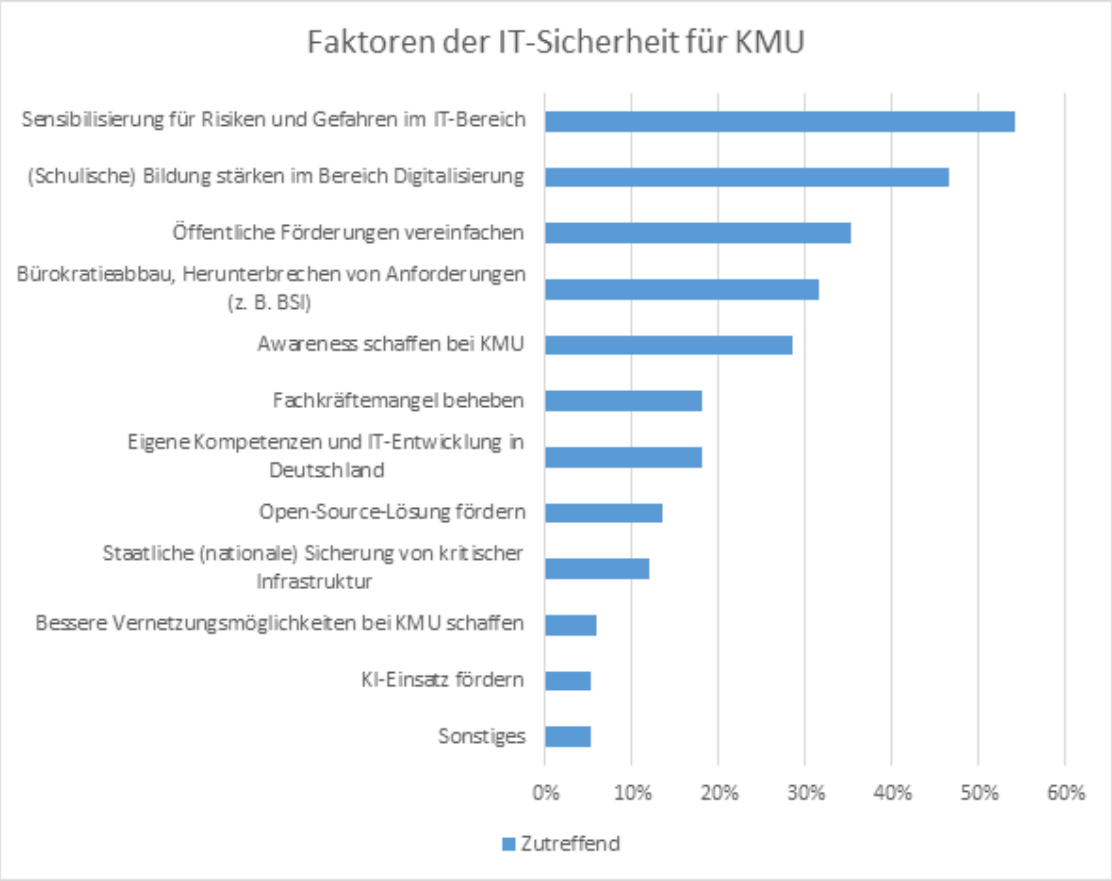

Abbildung 40 – Faktoren zur Verbesserung des IT-Sicherheitsniveaus bei KMU.

7.3. Wesentliche Erkenntnisse aus der qualitativen und quantitativen Befragung der IT-Dienstleister

7.3.1. Risikofaktor Mensch

Der Faktor Mensch ist nach wie vor als eines der größten Risiko- bzw. Sicherheitsfaktoren für die IT-Sicherheit von KMU anzusehen. Dies bestätigt sowohl die qualitative als auch die quantitative Befragung der IT-Dienstleister. Menschliches Verhalten prägt darüber hinaus auch – direkt oder indirekt – andere unternehmensrelevante Faktoren, wie die Anpassung/Optimierung von Organisationsprozessen oder die Kontrolle der Speicherung technischer Sicherheitsprotokolle. Dazu berichten Teilnehmende aus beiden Umfragen, dass KMU teilweise immer noch fälschlicherweise annehmen, dass sie kein lohnenswertes Ziel seien. Diese in der Regel subjektive Annahme deckt sich nicht mit den Erfahrungen vieler IT-Dienstleister.

Alle 25 interviewten IT-Dienstleister gaben an, dass sie konkrete Erfahrungen mit Angriffen bei KMU-Kunden gemacht haben. Mit fortschreitender Digitalisierung auch bei kleinsten KMU ist anzunehmen, dass der menschliche Faktor auch in Zukunft eine entscheidende Rolle beim IT-Sicherheitsniveau einnehmen wird. Insbesondere wenn nach Ansicht von 36% der quantitativ Befragten – im Vergleich zu anderen Bedrohungen für KMU – menschliches Versagen den mit Abstand größten Faktor ausmacht.[151] Darüber hinaus sehen 31% der IT-Dienstleister – im Vergleich des möglichen bzw. tatsächlich eingetretenen Schadens durch die jeweiligen Bedrohungen für KMU – den Faktor Mensch als für die größte Ursache für eintretende Schäden an.[152]

Daraus darf wohl geschlossen werden, dass weitere und intensivere Bemühungen, die Wahrnehmung für das Thema zu schärfen, notwendig sein werden. Gleichwohl stellt sich die Frage, in wie weit weitere Maßnahmen in diese Richtung zu einem zufriedenstellenden Sicherheitsniveau führen und welche Maßstäbe und Schwellenwerte (*threshold*) als ausreichend angesehen werden. Denn selbst dort, wo hinreichendes Bewusstsein vorhanden ist, kann es aufgrund von Zeitmangel und der Nicht-Sichtbarkeit von Datenverlusten weiter zu großen IT-Sicherheitslücken kommen.

7.3.2. Standardisiert vs. Spezifisches Produktportfolio

Die Ergebnisse aus beiden Umfragen zeichnen ein fragmentiertes Anbieterbild, das sehr unterschiedlich und abhängig von der Größe des IT-Dienstleisters ist. Bei der quantitativen Befragung bietet eine Mehrheit der Dienstleister einen Mix aus standardisierten und spezifisch angepassten Lösungen an (mit kleineren Abweichungen bei manchen der Kategorien). Die qualitativ Befragten streben dagegen mehrheitlich standardisierte Produkte an, da dann die Wartung und das Management auch frei durchführbar und ersetzbar bleibt.

[151] 25% Organisationsversagen, 20% Angriffe, 19% Technisches Versagen.
[152] 24% Technisches Versagen, 23% Angriffe, 22% Organisationsversagen.

7.3.3. MitarbeiterInnen mit spezifischer IT-Ausbildungen

In beiden Umfragen zeigt sich deutlich, dass IT-Dienstleister MitarbeiterInnen mit Ausbildungen bzw. einem Studium im Bereich der Informatik suchen. In der quantitativen Umfrage zeigt sich, dass für die Teilnehmenden eine spezifische technische Ausbildung als z. B. FachinformatikerIn noch wichtiger ist, als ein einschlägiges Studium der Informatik. Dies könnte auf das Gehaltsgefüge innerhalb der Unternehmen als auch die Gehaltsvorstellungen der Bewerber zurückgeführt werden. Das Gehalt von Berufseinsteigern nach einer Ausbildung dürfte tendenziell unter dem von akademischen Absolventen liegen.

Von steigender Bedeutung sind laut Aussagen vieler Interviewpartner duale Studiengänge, wobei sich bei den quantitativ Befragten ein eher uneinheitliches Bild darstellt. Die meisten der befragten IT-Dienstleister (43%) waren sich nicht sicher, ob ein duales Studium *eher wichtig* oder *eher unwichtig* bei der Auswahl und der Einstellung geeigneter MitarbeiterInnen für den IT- und IT-Sicherheitsbereich ist. Ein Grund dafür liegt sicherlich an der noch überschaubaren Anzahl an dualen Studiengängen in Deutschland und der damit verbunden geringen Anzahl an AbsolventInnen und dem Konzept im IT-Sicherheitsbereich allgemein.

Selbiges gilt für QuereinsteigerInnen, zu denen mehr als die Hälfte (52%) keine eindeutige Aussage dazu machen wollten oder konnten. Das Risiko, ungeeignete bzw. unqualifizierte KandidatInnen bei der Gruppe der QuereinsteigerInnen einzustellen, dürfte deutlich höher sein, als bei BewerberInnen mit einschlägiger Ausbildung, was dieses differenzierte Bild erklären könnte. Die Ergebnisse der qualitativen Umfragen zeigen jedoch, dass bei ausgewiesenem Interesse und Entwicklungspotenzial QuereinsteigerInnen auch gerne getestet und bei Eignung übernommen werden.

7.3.4. Neukundenakquisition/ Anbietermarkt

Unterschiede zeigen sich in der Vorgehensweise bei der Neukundenakquisition. Die qualitativ Befragten gaben an, dass sie aktiv auf KMU-Kunden durch u.a. Anzeigen und in-House Messen zugehen. Nur bei den kleinsten regionalen IT-Dienstleistern scheint die *Mund-zu-Mund Propaganda* entscheidend. Empfehlungen bei der Neukundenakquisition wurden bei der quantitativen Umfrage mit großem Abstand am häufigsten genannt. Über Verbände und Netzwerke scheinen IT-Dienstleister auch einen signifikanten Anteil an Neukunden zu gewinnen (44%). Dabei ist zu berücksichtigen, dass viele TeilnehmerInnen der vorliegenden Befragung über Verbände erreicht wurden und sie vermutlich diese Verteiler auch im beträchtlichen Maße zur Neukundenakquisition einsetzen. Diese werden von den IT-Dienstleistern ebenso als Informationsquellen zu aktuellen Sicherheitsproblemen genutzt.

Insgesamt scheint die Neukundenakquisition keine besondere Herausforderung für IT-Dienstleister zu sein. Dies zeigt sich auch durch Aussagen und Ergebnisse aus beiden Umfragen: insbesondere kleinste KMU sind als Kunden am wenigsten interessant. Die angespannte Situation auf dem Arbeitsmarkt, gepaart mit einer hohen Nachfrage nach IT-Dienstleistungen, erfordert den möglichst effizienten Einsatz von Ressourcen. Dies kann dazu führen, dass Aufträge nicht angenommen oder weniger lukrative Anfragen ausgeschlagen werden.

Festzuhalten ist, dass IT-Dienstleister einen entscheidenden Beitrag zur Steigerung des Sicherheitsniveaus in KMU leisten. Bezüglich der Zusammenarbeit der IT-Dienstleister mit KMU zur Fragestellung der Studie und der Rolle der IT-Dienstleister für mehr Sicherheit bei KMU, liegen nur wenige Analysen vor. Gleiches gilt auch für die Attraktivität der Kundengruppe der KMU für IT-Dienstleister mit IT-Sicherheitsdienstleistungen. Unstrittig ist nach unseren Studienergebnissen die hohe Nachfrage nach IT- und IT-Sicherheitsdienstleistungen durch die KMU.

Der Anbietermarkt der IT-Dienstleister zeichnet sich dadurch aus, dass

- bei qualifizierten IT-Dienstleistungen für KMU ein Nachfrageüberhang besteht,
- der Bedarf, insbesondere bei Vorfällen und besonderen Ereignissen, dringlich ist (zunehmende Digitalisierung ist insofern auch als besonderes Ereignis zu sehen),
- der Anbieter über höhere Fachkenntnisse verfügt,
- KMU als Nachfrager vom IT-Dienstleister als Anbieter abhängig ist.

Für die IT-Dienstleister, die sich im Marktsegment einer hohen Nachfrage und sehr knapper fachlicher Ressourcen bewegen, bietet das KMU-Segment - nach unseren Erkenntnissen - nicht immer ein ausreichend attraktives und priorisiertes Marktsegment. Die KMU stellen zudem hohe Anforderungen an die branchen- und fachspezifische Qualifikation der Dienstleister. Gerade in der Akquisition von IT-Dienstleistungen spielt Vertrauen als wichtiges Kriterium für eine erfolgreiche Zusammenarbeit eine besondere Rolle.

Aus Sicht der Nachfrager (KMU) ist es insofern von besonderer Bedeutung, eine qualifizierte Anforderungsanalyse und Auswahl geeigneter IT-Dienstleister treffen zu können.

7.3.5. Öffentliche Förderung

Zwar scheinen viele verschiedene Fördermaßnahmen von Bund und Ländern im Bereich der IT-Sicherheit bekannt zu sein, insbesondere das mit großem Abstand am häufigsten genannte Förderprogramm „go-digital“ des BMWi, allerdings scheinen viele KMU die für sie relevanten Fördermöglichkeiten aufgrund der Vielzahl an Programmen des Bundes und der Länder nicht bestimmen zu können. Die Übersicht geht sprichwörtlich verloren. Dazu kommen oftmals aus Sicht der IT-Dienstleister komplizierte Antragsverfahren und teilweise lange Antragsphasen, die abschreckend wirken.

7.3.6. Transferstelle zur Förderung von IT-Sicherheit

Während der Projektlaufzeit dieser Studie hat das BMWi mit der Transferstelle IT-Sicherheit im Mittelstand (TISiM) eine Initiative gestartet, die sich unmittelbar an kleine und mittlere Unternehmen wendet und konkrete Lösungen erarbeitet. TISiM soll unter anderem KMU dabei unterstützen aus einer Vielzahl von bestehenden IT-Dienstleistungen und IT-Produkten die jeweils für sie passenden Angebote leichter zu finden. Für die Zielgruppe der KMU sollen mithilfe

von TISiM konkrete Aktionspläne und Anleitungen erarbeitet werden, die eine praktikable Umsetzung und somit Erhöhung der IT-Sicherheit ermöglichen. Mit TISiM-Regional werden zudem regionale Ansprechstellen etabliert werden.

Durch TISiM werden somit die folgenden Anforderungen aufgegriffen:

- Informationsbereitstellung zu IT-Sicherheitsthemen mit fachlichen Bezug und KMU-Orientierung.
- Unterstützung bei der Auswahl geeigneter Angebote und Dienstleistungen unter Berücksichtigung regionaler Aspekte der Nachfrager (KMU).
- Verbesserung der Informationen zu Fördermöglichkeiten und -programmen für mehr IT-Sicherheit bei KMU (bundesweite und regionale Programme).
- Sensibilisierung der KMU.

Die TISiM wurde sowohl in der Befragung der IT-Dienstleister als auch der KMU zu Netzwerken und Informationsquellen (siehe Abbildung 39 & Abbildung 54) noch nicht ausreichend sichtbar. Dies wird sich sicherlich mit zunehmenden Vernetzungs- und Bekanntheitsgrad verbessern. Die notwendige Funktion einer Anlaufstelle und auch Hotline bei IT-Vor- und Notfällen kann TISiM nicht übernehmen.

Die ebenfalls notwendige operative Hilfe in akuten IT-Vorfällen stellt eine zusätzliche erforderliche Aufgabe dar, die momentan in einem BSI Projekt aufgegriffen wurde.

8. Befragung der KMU

Wie bereits für die Befragung der IT-Dienstleister wurden auch an dieser Stelle die Rahmenbedingungen für die Befragung der KMU mit dem Auftraggeber festgelegt. Gemeinsam wurden die übergeordneten Fragestellungen für die Befragung der KMU definiert, die Vor- und Nachteile verschiedener Befragungstechniken erörtert und die Samplegrößen festgelegt. In den nachfolgenden Abschnitten werden die Festlegungen erläutert.

8.1. Erarbeitung eines Interviewleitfadens

Im Rahmen dieses Arbeitspakets wurde zunächst ein Interviewleitfaden erarbeitet. Aus den Erkenntnissen der Marktbetrachtung und den Hintergrundgesprächen mit den IT-Sicherheitsfachleuten wurde analysiert, welche Themen sich für eine Befragung zum Umgang mit IT-Sicherheit besonders eignen.

8.2. Qualitative Befragung der KMU

Für die qualitative Befragung der KMU wurde zunächst ein Sampling (siehe Abschnitt 4.2) erstellt, welches sich an der Definition der Wirtschaftsbereiche[153] des Instituts für Mittelstandsforschung (IfM Bonn) orientiert. Gegliedert nach Größe (Kleinstunternehmen bis 9 MitarbeiterInnen, Kleinunternehmen 10-49 MitarbeiterInnen und mittlere Unternehmen 50-499 MitarbeiterInnen) und Branche (Baugewerbe; Bergbau, Energie-, Wasserversorgung, Entsorgung; Finanz- und Versicherungsdienstleistungen, Grundstücks- und Wohnungswesen; Handel, Gastgewerbe; Personenbezogene Dienstleistungen; Unternehmensnahe Dienstleistungen; Verarbeitendes Gewerbe sowie Verkehr, Information und Kommunikation) war eine Anzahl von jeweils zwei KMU quotiert (siehe Tabelle 4 in Abschnitt 4.2). Die Auswahl der interviewten KMU erfolgte dann auf Basis von Kontakten des Auftragnehmers, Adressbestände der IHKn sowie relevanter Unternehmensnetzwerke. Anschließend wurde die qualitative Befragung der KMU mittels Interviewleitfaden und auf Grund der COVID-19-Pandemie fast ausschließlich telefonisch durchgeführt. Genau wie bei der Befragung der IT-Dienstleister wurden die Interviews offen geführt und der Interviewleitfaden diente den Interviewenden lediglich als Gesprächsleitfaden. Daher arbeitete der Leitfaden (siehe PDF Anhang) vornehmlich mit Gesprächsaufforderungen und nicht mit Fragen. Das offene Verfahren sorgte dafür, dass sich die befragten Unternehmen wichtig und ernst genommen fühlten.

Die qualitative Befragung wurde mit demselben Wortlaut vorgestellt wie bei der Befragung der IT-Dienstleistungsunternehmen:

[153] Wirtschaftsbereichsstruktur der KMU in Deutschland, https://www.ifm-bonn.org/statistiken/mittelstand-im-einzelnen/#accordion=0&tab=1, Zugriff v. 10.03.2020.

> *Im Auftrag des Bundeswirtschaftsministeriums führen wir eine Studie zur IT-Sicherheit im Bereich der kleinen und mittleren Unternehmen in Deutschland durch. Ziel der Studie ist es, eventuell bestehende Lücken in der Kommunikation zwischen Dienstleistern und potenziellen Kunden zu schließen und somit für mehr IT-Sicherheit am Standort Deutschland zu sorgen.*

Neben statistischen Daten wie Name, Alter, Größe und Sitz(e) des Unternehmens, waren die Schwerpunkte der Interviews die Punkte:

1. Wahrgenommene (IT-)Bedrohungen und Risiken der IT-Sicherheit in Ihrem Unternehmen
2. Ihre Arbeitsorganisation und -prozesse in der Zusammenarbeit mit IT-Dienstleistern
3. Qualifikation und Weiterbildung Ihrer IT-Zuständigen
4. Einsatz technischer Lösungen (Was nutzen Sie bereits zum Schutz Ihres Unternehmens?)
5. Auswahl IT-Dienstleister

Darüber hinaus wurde vollständig offen abgefragt, ob es wichtige Bereiche zum Thema IT-Sicherheit gibt, die bisher in dem Gespräch nicht hergeleitet wurden. Aus Zeitgründen und auf Grundlage der Projektkalkulation erfolgte keine Transkription, sondern lediglich eine stichpunktartige Protokollierung und eine doppelte Aufzeichnung der Interviews, aus der dann bezüglich der oben genannten Bereiche Kategorien abgeleitet und die Kernergebnisse in einer Tabelle zusammengetragen wurden.

Die in Abschnitt 9.1 folgenden Auswertungen basieren auf 50 Interviews.

8.3. Generierung eines quantitativen Online-Fragebogens

Wie bereits im vorigen Abschnitt erläutert, wurde aufbauend auf den Erkenntnissen der offen geführten Interviews die Leitfragen in einen standardisierten Online-Fragebogen überführt, der an alle verfügbaren Adressen der Datenbestände des Konsortiums elektronisch versendet wurde. Rücklaufsichernde Maßnahmen wie Nachfassaktionen und ggf. Telefonbefragungen wurden zur Qualitätssicherung genauso eingeplant, wie Pretests der Instrumente. Der quantitative Online-Fragebogen für die IT-Dienstleister wurde inhaltlich mit dem Auftraggeber abgestimmt und von diesem freigegeben.

8.4. Quantitative Befragung der KMU

Die Online-Befragung wurde auf der u.a. Projektseite der NKMG veröffentlicht[154] und über vorab identifizierte und angesprochene Netzwerke sowie direkte Adressen des Studienteams elektronisch verteilt.

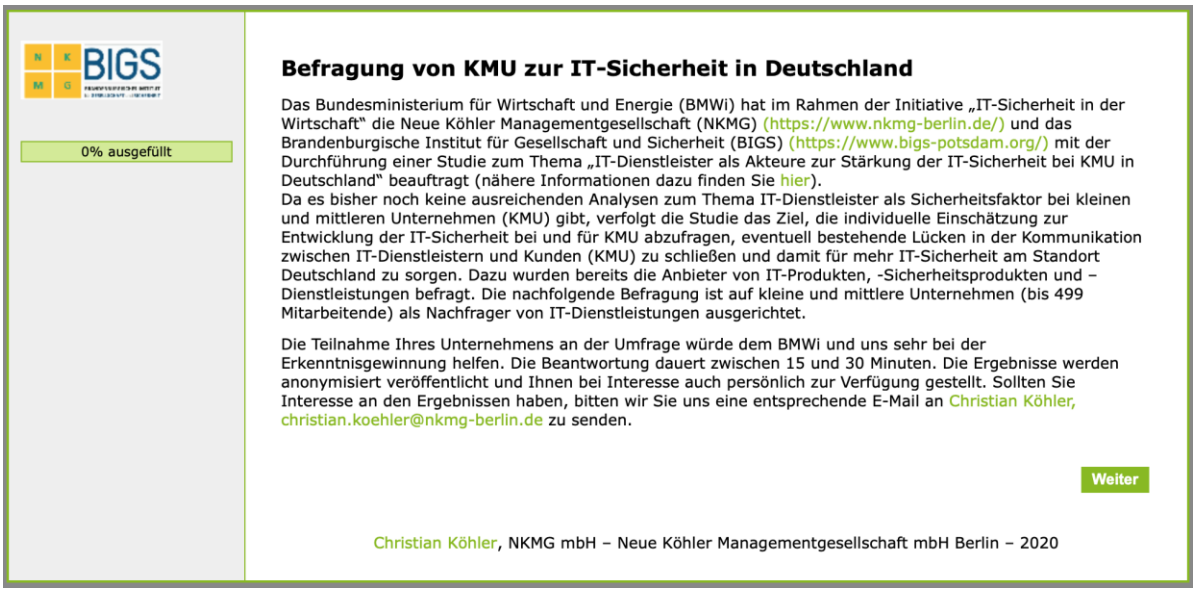

Abbildung 41 – Startansicht des Online-Fragebogens für die quantitative Befragung der KMU,

DOI: https://www.soscisurvey.de/KMUITSIC/

Bei der quantitativen Befragung der KMU mittels Online-Fragebogen (siehe PDF Anhang) wurde mit geschlossenen Fragen gearbeitet, wobei die Befragten mithilfe von Likert-Skalen ihre Zustimmung, Bedeutung oder Ähnliches einschätzen mussten. Wie im Falle der quantitativen Befragung der IT-Dienstleister, wurde für diesen online-Fragebogen ebenfalls ein Begleitschreiben vom BMWi aufgesetzt. Auch dieses ist dem Anhang zu entnehmen.

Um ein breites Spektrum an KMU zu erreichen, griff das Konsortium auf ihr breites Netzwerk zurück. Hierzu wurden folgende Multiplikatoren, wie aus der Tabelle 7 zu entnehmen ist, herangezogen. Ein umfangreiches Clipping ist im Anhang vorzufinden. Über die Verbände und Netzwerke der NKMG wurde der Befragungslink auch mithilfe von Social-Media-Kanälen verteilt (Twitter, LinkedIn, XING).

[154] Veröffentlichung der Online-Befragung der KMU über die Projektseite der NKMG, https://www.nkmg-berlin.de/projekte/befragung-zur-studie-it-sicherheit-des-bmwi/kmu-befragung

Tabelle 7 Multiplikatoren zur Verteilung des KMU-Befragungslinks

Institution (Multiplikatoren) zur Verteilung des Befragungslinks zur KMU-Befragung	
Bundesverband Mittelständische Wirtschaft e.V. (BVMW)	HTW - Gründernetzwerk
BIGS - Newsletter	Innovatives Brandenburg (IB)
DIHK	Innovative Hauptstadtregion (IH), Berlin
Digitale Hauptstadtregion	IH Cluster IKT, Medien und Kreativwirtschaft
European Aviation Security Center e.V.	IH Cluster Energietechnik
HWK Rheinhessen	IH Cluster Optik und Photonik Berlin Brandenburg
HWK Osnabrück-Emsland-Grafschaft Bentheim	IHK Berlin
HWK Aachen	IHK Potsdam
HWK Magdeburg	IBWF Institut e.V.
HWK für Schwaben	Kompetenzzentren Mittelstand Digital
HWK Dortmund	NKMG Projektseite
HWK Halle (Saale)	Transferstelle IT-Sicherheit im Mittelstand (TiSIM)
HWK Kassel	Zentralverband des Deutschen Handwerks
HWK Oberfranken	DIGITALWERK Brandenburg

Die mit dem Auftraggeber vereinbarte Zielstellung wurde auf eine Rücklaufquote von mindestens 100 Unternehmen vereinbart. Im Befragungszeitraum vom 17.07.2020 bis 21.10.2020 haben insgesamt 176 KMU an der Online-Befragung teilgenommen, von denen 89 die Fragebögen vollständig ausfüllten.

9. Studienergebnisse aus der Befragung der KMU

9.1. Studienergebnisse der qualitativen Befragung der KMU

Nachfolgend werden die wesentlichen Erkenntnisse der qualitativen KMU- Befragung zusammengefasst. Hierzu werden die KMU in einem ersten Schritt, entsprechend ihrer Aussagen, in vier Kategorien eingeteilt:

- KRITIS-nahe KMU oder sehr IT-affine Dienstleister,
- KMU, die Teil einer größeren Muttergesellschaft sind,
- mit Standards arbeitende Händler und Servicebüros sowie
- Kleinstdienstleister.

In einem zweiten Schritt folgt eine übergreifende Auswertung der Befragungsgruppe der KMU, unterteilt in folgende Unterpunkte:

- Suche und Auswahl der IT-Dienstleister,
- Allgemeine Problembeschreibung,
- Offene Punkte und
- Weitere Punkte.

9.1.1. KRITIS-nahe KMU oder sehr IT-affine Dienstleister

Diese KMU Gruppe zeichnete sich durch eine am aktuellen Wissenstand orientierte Aufstellung ihres Geschäftsmodells und ihrer Informationstechnik aus. Dieser Status wird durch die Beschaffung regelmäßiger Informationen zu IT- und IT-Sicherheitsthemen beibehalten. Bei dieser KMU-Gruppe fällt des Weiteren auf, dass das Konzept der IT-Sicherheit von Anbeginn ihrer strategischen Ausrichtung mitgedacht wird. Dabei wird die Technik, laut Aussage der befragten KMU, kontinuierlich auf dem aktuellen Stand gehalten und entsprechend ihrer Kerngeschäftsbedürfnisse skaliert.

Der Ort zur Speicherung ihrer Daten wird häufig bewusst in Deutschland ausgewählt. Die von diesen KMU verwendeten Softwareprodukte, die in überwiegender Zahl von ausländischen Anbietern bereitgestellt werden, dürfen ausschließlich für den deutschen bzw. europäischen Markt bestimmt sein. Hierdurch wird sichergestellt, dass die Programme mit laufenden Updates auf dem aktuellen Stand gehalten werden, im Gegensatz zu sogenannter „Grauware“. Bezogen werden diese Produkte vorzugsweise über regionale Anbieter.

Ferner findet bei dieser Gruppe ein reger Austausch in Verbänden oder über die Einbeziehung von Fachleuten statt. In Bezug auf die Unterstützung durch staatliche Einrichtungen und Programme, kritisiert diese befragte KMU-Gruppe oftmals, dass öffentliche Fördermaßnahmen ihre tatsächlichen Arbeitsbedingungen und Infrastrukturprobleme nicht hinreichend berücksichtigen.

9.1.2. KMU als Teil einer Muttergesellschaft (Versicherungen, Autohäuser, Universitätsausgründungen)

KMU, die unter dem Dach einer Holding- oder größeren Muttergesellschaft operieren, tendieren in unserer Befragung zu einer hohen Selbsteinschätzung bezüglich der Aufstellung ihrer IT-Sicherheitsarchitektur. Beispielsweise wurden von den befragten KMU wiederholt Aussagen getroffen: „dass sie der Konkurrenz in Sachen IT 10 Jahre voraus" seien. Prozesse, Hard- und Software-Lösungen dieser Gruppe orientieren sich mehr oder weniger an geltenden Standards und werden auf dem aktuellen Stand gehalten. Die Richtlinien und Standards werden dabei zumeist vom Dachunternehmen vorgegeben.

Nichtsdestotrotz müssen manche der getroffenen Entscheidungen innerhalb dieser KMU-Gruppe kritisch betrachtet werden. Oftmals wird für wichtige IT-Dienstleistungen der Service und das Produktportfolio von Ein-Personen-Betrieben beansprucht. Dies hat zur Folge, dass Abhängigkeiten geschaffen werden, die sich stark negativ auf das operative Geschäft auswirken können. Zumeist wird bei diesem Typus der KMU einer Back-up Strategie nicht genügend Beachtung geschenkt. Es muss bei dieser KMU-Kategorie davon ausgegangen werden, dass sie sich zu unkritisch mit dem Thema Datenschutz und IT-Sicherheit auseinandersetzt, da keine hinreichenden Überlegungen zur Sicherheit der Anwendungen und zur Speicherung angestellt werden.

Bei dieser Gruppe liegen Informationen zu Datenschutz und IT-Sicherheit oftmals in der Dachorganisation oder bei der Geschäftsführung vor, werden allerdings nur auf unregelmäßiger Basis oder fachlich unzureichend weitergegeben. Bezeichnend für diese KMU-Gruppe ist, dass sie nur an bestimmten Fördermaßnahmen interessiert ist. An dieser Stelle wird von einigen KMU Kritik an überbordender bzw. teils gedoppelter Bürokratie geäußert. Es wird dabei auf die bereits in ihrem Geschäftsfeld auftretenden administrativen Hürden hingewiesen.

9.1.3. Mit Standards arbeitende Händler und Servicebüros (z.B. Datev nutzende IT-affine Steuerbüros, Kanzleien, Baustoffhändler)

Diese KMU Gruppe weist zumeist eine an das eigene Kerngeschäft gut angepasste IT und IT-Sicherheit auf. Ihre Hard- und Software sowie IT-Infrastruktur sind entsprechend der Verwendung (z.B., Steuerung aus der Ferne) oder an den Erfordernissen (z.B. Baustellenbetrieb) und unter Berücksichtigung des Preises dem Unternehmen angepasst. Diese Unternehmen führen eine ständige Überprüfung von Neuerungen durch und evaluieren, ob sie der wirtschaftlichen Ausrichtung des Unternehmens förderlich sind. Die IT muss robust aufgestellt sein.

Auch unter dieser Gruppe wird Kritik an durch Datenschutz-, Melde- und Statistikanforderungen verursachte Mehrarbeit geäußert. Hier wird jedoch ein pragmatischer Ansatz zur Lösungsfindung gesucht. Es wird erkannt und akzeptiert, dass der Datenschutz für innere Zwecke durchaus sinnvoll ist. An Fördermaßnahmen besteht ein reges Interesse. Die Beantragung wird jedoch häufig für umständlich gehalten. Hierzu besteht ein reger Austausch an Informationen innerhalb diverser Branchenverbände, die eine agile Arbeitsweise unter ihren Mitgliedern fördern.

9.1.4. Kleinstdienstleister (Franchise, Gestalter, Architekten, konventionelle Dienstleister, Servicebüros)

Die letzte KMU-Gruppe wird durch eine oft jahrzehntelange Routine charakterisiert, die auch bei ihren Kunden vorzufinden ist. Dadurch sind Veränderungen, auch der IT, nicht ohne weiteres umzusetzen. Von dieser Einstellung sind oftmals auch KMU-Neustarter betroffen. Ferner ist bei dieser Gruppe auch eine Zentrierung auf die Geschäftsführung zu beobachten. Diese KMU berichteten von einer permanenten Arbeitsüberlastung, da ihre IT nicht von vornherein mitgedacht worden ist. Eine entsprechende Ausbildung der MitarbeiterInnen zur Beseitigung aufkommender Probleme ist nicht oder nur in ungenügender Form vorhanden.

Bezeichnend für diese unzureichende Aufstellung der Unternehmen und das fehlende Verständnis sind beispielsweise nachfolgende genannte Auswege: „Ich habe einen Apple-Computer - der ist sowieso sicher.“, „Ich schreibe kaum E-Mails.“, „Es muss sowieso alles auf Papier abgegeben werden.“. Einige KMU ließen durch folgende Äußerungen einen aufgebauten Fatalismus erkennen: „Das ist eh nicht aufzuhalten. Sogar meine Fitnessuhr sendet Umgebungsdaten nach China.“, „Bill Gates weiß am besten, wie seine Systeme am Laufen gehalten werden.“. Dies wird auch durch den Umstand bestätigt, dass teilweise keine IT-Dienstleistungen in Anspruch genommen werden. Der Umgang mit dem Datenschutz ist in vielerlei Hinsicht unzureichend. Oftmals findet keine Trennung von Arbeits- und Privatleben statt. Das zeigt sich anhand der Äußerung, dass man sich auf das Kerngeschäft mit „leichtem Tunnelblick“ konzentriert.

9.1.5. Übergreifende Auswertungen

Die übergreifende Auswertung der qualitativen Befragung der KMU umfasst insbesondere die folgenden drei Aspekte: Entscheidungskriterien zur Suche und Auswahl eines passenden Dienstleisters, allgemeine Problembeschreibung, die sich für diese Unternehmen auftun und weitere offene Punkte, die im Hinblick auf die Informationsbeschaffung ausgedrückt wurden.

9.1.5.1. Auswahl der IT-Dienstleister

Die KMU-Gruppen der Kategorien zwei und drei weisen bezüglich der Auswahl der IT-Dienstleister eine ähnliche Herangehensweise auf. Die erste Gemeinsamkeit dieser KMU bezieht sich auf deren Inanspruchnahme von IT-Dienstleistungen, die in der Regel ein/e einzelne/r MitarbeiterIn (entweder ein/e Soloselbstständige/r oder ein/e dedizierte/r MitarbeiterIn eines IT-Kleinstunternehmens) erbringt. Diese/r oftmals als „Ein-Personen-RetterIn“ bezeichnete MitarbeiterIn ist vorzugsweise durch private, direkte oder gesellschaftliche Beziehungen in diese Position gekommen und hat sich durch sein langes Mitwirken im Unternehmen unverzichtbar gemacht. Diese IT-Dienstleister werden dabei selten von den KMU hinterfragt. Erst wenn sich ein drohendes Ausscheiden des IT-Dienstleisters aus dem Unternehmen abzeichnet oder die Leistung des IT-Dienstleisters nicht länger in Anspruch genommen werden kann, werden von Seiten dieser KMU entsprechende Maßnahmen ergriffen. Diese IT-Dienstleister haben in der Vergangenheit häufig

das Geschäft der Unternehmen im Aufbau betreut und dabei ihre IT-Fähigkeiten proportional an diese Erfordernisse angepasst. Ferner hat sich eine Wechselbeziehung zwischen dem IT-Dienstleister und internen MitarbeiterInnen, die beispielsweise für die IT im KMU zuständig sind, entwickelt. So werden diese internen MitarbeiterInnen oftmals durch die IT-Dienstleister bei der Erbringung von kleinen Installationen und Back-Ups angelernt.

9.1.5.2. Übergreifende Problembeschreibung der KMU-Gruppe zur IT-Sicherheit

Aus den Äußerungen der KMU-Befragung werden übergreifende Probleme erkennbar. Unter anderem gaben die befragten KMU aus den Kategorien zwei bis vier an, dass sie einer „Augen zu und durch" Mentalität folgen würden. Demnach verlassen sie sich beispielsweise auf die Unterstützung kostenloser Software, wie Online-Auswertungsprogramme. Gleichzeitig findet unter diesen KMU keine ausreichende Trennung der verwendeten Daten aus Arbeits- und Privatleben statt. Oftmals wurde angegeben, dass es keinerlei Kenntnis über die fachliche Expertise des eingestellten IT-Angestellten in den untersuchten KMU gibt.

Wenn zum Teil besondere Anforderungen der befragten KMU nicht erfüllt werden können, so wird von einer kompletten Resignation hinsichtlich dieses Vorhabens berichtet. Um dem zu begegnen, wird alternativ auch der Einsatz von Anwendungen erwähnt, welche möglicherweise den Datensicherheitsanforderungen des Gesetzgebers nur in ungenügender Weise entsprechen. Dabei wird gelegentlich von Anwendungen und Software Gebrauch gemacht, wie beispielsweise WhatsApp, ohne jedoch die technisch mögliche Zusatzsicherung zu berücksichtigen. An der Stelle wurde von den befragten KMU angemerkt, dass statt der Sicherheit bei der Auswahl der Anwendungen, vorwiegend der Beliebtheit von Anwendungen der Vorzug gegeben wird.

Laut deren Aussage würde die Bereitstellung von mehr Informationen zu heimischen oder europäischen Anwendungen bei der Auswahl von IT-Dienstleistungen helfen. Dies wird durch Aussagen vieler KMU bekräftigt, wonach die Beschaffung oder Erbringung von IT-Dienstleistungen und -lösungen sich gegenteilig der Beschaffung beispielsweise von Konsumentenprodukten verhalten. Die Komplexität und Individualität von IT-Lösungen machen eine Beschaffung schwieriger. Dazu merkten TeilnehmerInnen der Befragung an, dass sich bei internationalen Geschäften die großen Anbieter wie Apple, Google und Microsoft nicht automatisch als die besseren erweisen. Diesbezüglich wird von diesen KMU eine Vorreiterrolle von staatlichen Organen erwartet. Hier könnten die gesammelten Informationen und Erfahrungen aus den Anwendungen, laut Aussagen der KMU, auch in Schulen und Universitäten genutzt werden. Dies würde einen sinnvollen und skalierbaren Einbau dieser Kompetenzen bei Existenzgründungen ermöglichen. Pilotprojekte sollten dabei klein und agil ausgestaltet werden.

9.1.5.3. Forderungen der KMU zu Digitalisierungsfragen und Informationsversorgung

In diesem Abschnitt hatten die KMU die Gelegenheit auf offene Probleme näher einzugehen. Daraus hat sich unter anderem ergeben, dass das BSI als Kontaktstelle für einige der Befragten eine zu hohe Ansprechhürde darstellen

würde. Inwiefern sich diese Hürden bei der Kontaktaufnahme manifestieren, wurde von den befragten KMU leider nicht weiter präzisiert.

Des Weiteren wurde von einigen KMU darauf hingewiesen, dass ihnen nicht genügend skalierbare Sicherheitsmodelle bekannt sind. An der Stelle könnten sie sich eine direkte Ansprache über Branchenverbände, Industrie- und Handelskammern (IHK) und Handwerkskammern (HWK), Start-Up-Beratungen oder Franchisegebern vorstellen. Statt einer teuren Beraterförderung, die oftmals durch die öffentliche Hand in Aussicht gestellt wird, wäre ihrer Meinung nach eine einfachere Hinzuziehung von regionalen IT-Dienstleistern und Coaches wünschenswert. Dies sollte am besten anhand von grundlegenden Anleitungen, Listen und Richtlinien von einer zentralen Stelle bereitgestellt werden. Dieser Wunsch sei unter anderem dem Umstand geschuldet, dass die Qualitäten der Förderungsinformationen und der Nachrichtenbeschaffung regional höchst unterschiedlich ausgestaltet sind.

Es wurde ferner angemerkt, dass sich sicherheitsaffine Firmen beim BSI und sogar im Ausland informieren. Diese Möglichkeit der Informationsbeschaffung sollte laut Aussage auch für KMU auf nationaler Ebene vorhanden und in skalierbarer Form abrufbar sein. Fördermaßnahmen und Informationen zu Förderungen würden zwar auf Bereiche abzielen, in denen innerhalb der KMU erhebliche Wissenslücken herrschen. Das Beantragungs- und Nutzungspotential kann dennoch von vielen nicht in Anspruch genommen werden. Selbst IT-affin aufgestellte KMU sollen häufig nicht in der Lage sein, die Fördermaßnahmen mit ihren Entwicklungsprogrammen zu synchronisieren. Insbesondere werden hierbei Behördenabläufe als Innovationsverhinderung genannt. Vorgegebene Zeitfenster, Anwendungen oder mehrfache Antragseingaben bzw. Statistiken können in der geforderten Form nicht eingehalten bzw. vorgelegt werden. Im Hinblick auf die Covid-19 Pandemie wurde teils Verwunderung darüber geäußert, dass einige berechtigte Verbote plötzlich ausgesetzt werden konnten, während andere Vorschriften, die nicht als entscheidend angesehen werden, weiterhin akribisch kontrolliert wurden.

Zuletzt wurde mehrmals die Notwendigkeit zur ernsthaften Umsetzung einer Digitalisierungsagenda, wonach eine deutsche bzw. europäische Infrastruktur geschaffen werden sollte, zum Ausdruck gebracht. Diese sollte die Themen Bildung und Fortbildung umfassen und dabei eine Vorreiterrolle einnehmen. Informationen zu einer nationalen oder europäischen Vorgehensweise sollten vorliegen. Die Umsetzung sollte agil und lokal durchgeführt werden können. All diese Maßnahmen sollten dazu beitragen, ein Bewusstsein für diese Thematik zu schaffen, um damit fatalistische Einstellungen gegenüber IT-Sicherheit oder absolute Sicherheitsgefühle zu verhindern.

Wie zuvor in der Kategorisierung der KMU bereits beschrieben, befinden sich einige KMU unter der Kontrolle eines großen Mutterkonzerns bzw. einer Mutterorganisation, der die IT-Infrastruktur und die in Anspruch zu nehmenden Dienstleistungen vorgibt. Die von diesen Großunternehmen abhängigen KMU halten diese Lösungen für zumeist wegweisend und nicht anzweifelbar. Branchenlösungen für IT-Dienstleistungen ähneln im Charakter nicht selten dem Branchenimage. So werden beispielsweise Lösungen im Baugewerbe oft vom Entwurf bis zur Fertigstellung der Bauwerke mitgedacht und nach speziellen Bedürfnissen, auch robust, ausgestaltet. Auf diese Weise lassen sich Sonderlösungen leichter einbeziehen und die verwendeten Geräte und Softwarelösungen, je nach Anforderungen des Arbeitsortes, up- und auch downgraden (z.B. bei Outdoornutzung mit schwierigen Sicherheitsbedingungen).

Personennahe IT-Dienstleistungen von gehobenem Renommee und mit ausgeklügelten Lösungen weisen wiederum eine Vielzahl an Angeboten für ihre Kunden auf. Die Nutzung dieser Angebote ist dabei vergleichbar mit der Möglichkeit, Zusatzausstattungen, wie es in der Automobilindustrie üblich ist, hinzuzubuchen. Diese Hinzubuchungen erweisen sich aber oftmals als teuer und schwerfällig. Dies ist insbesondere dann der Fall, wenn Anpassungen an sich ändernde Rechtsvorgaben veranlasst werden müssen. Es wurde konstatiert, dass es im Kommunikationssektor, vor allem im digitalen Bereich, eine Vielzahl von Lösungen und Anbietern gibt. Dabei wurden folgende zwei Probleme explizit beschrieben:

(1) Es wird von einzelnen Branchen berichtet, dass viele unterschiedliche Dienstleister aus Kosten-Optimierungsgründen mit Teilaufgaben betraut werden. Dabei kommt es auf allen Seiten nicht selten zu Kompatibilitätsproblemen.

(2) bei Kommunikationsprodukten, die in ein materielles Produkt münden (z.B. Druckprodukt), befindet sich der „Flaschenhals“ in der Begrenzung der Verarbeitbarkeit von Software durch die Produktionsmaschinen.

Gesetzliche Vorgaben und Maßnahmen in Sachen IT-Sicherheit werden insgesamt von den KMU als durchaus sinnvoll erachtet. Als Grund wird beispielhaft angeführt, dass die unter „KRITIS“ und dem IT-Sicherheitsgesetz laufenden Branchen, technisch und IT-Sicherheitstechnisch nach aktuellem Stand der Anforderungen arbeiten müssen und damit gut aufgestellt sind. Die anderen Branchen müssten, das aus ihrer Sicht „unsichtbare und schwer greifbare“ Thema der IT-Sicherheit im Auge behalten. Die Vorgaben und der bürokratische Aufwand werden oft als hinderlich oder als unüberwindbare Hürde im Arbeitsalltag angesehen. Einige KMU sind sogar der Auffassung, dass sie sich außerstande sehen, sich mit den gesetzlichen Vorgaben auseinanderzusetzen. Skalierte und dem jeweiligen KMU-Kerngeschäft angepasste Regelungen werden dringend gewünscht. Neben einer Anpassung der Rahmenbedingungen durch den Gesetzgeber und mithilfe technischer Standards, wird eine praktikable und anpassungsrobuste Lösung, die sich branchenintern entwickelt, als wichtig erachtet. Ferner müsste laut Aussage der befragten KMU vermittelt werden, dass IT und IT-Sicherheit in der heutigen Zeit in jeder Branche von Beginn an mitgedacht werden sollte (Stichworte “security by design und security by default”). Diese Vorgehensweise wurde als notwendig empfunden, da selbst die vermeintlich traditionelle Produktion in digitale Prozesse und Umgebungen eingebettet ist.

Aus den Interviews lässt sich ein weiterer interessanter Punkt in Bezug auf den Fachkräftemangel bei IT-Dienstleistern erkennen. Während viele IT-Dienstleister oder RecruiterInnen für interne IT-Abteilungen auf „Google-ähnliche Erwachsenenspielplätze“ mit Lounges und Experimentalküche als Lockmittel für ihre Anwerbung setzen, sind viele gefragte IT-lerInnen eher an einem individuell zusammengestellten Kundenportfolio interessiert. Dieses Portfolio kann kleine, regionale, und durch gute persönliche Erfahrungen ausgezeichnete KMU umfassen. Aber auch ferngewartete Einzelunternehmen und Branchenführer, die durch in Arbeitsgruppen organisierte FreelancerInnen betreut werden. Persönliche Beziehungen und fachliches Interesse sind selbst in Branchen ausschlaggebend, in denen permanent neu ausgeschrieben werden muss. Es lässt sich aus den getroffenen Aussagen der KMU zu der großzügigen Gehaltspolitik der Branchenführer nicht automatisch darauf schließen, ob sich ein Nachteil für die KMU in Sachen IT-Sicherheit ergibt.

Zwei grundsätzliche Punkte können aus den Interviews noch angemerkt werden:

1. KMU haben Zweifel zum Ausdruck gebracht, wonach sie die IT-Sicherheit von Anbeginn in ihrer strategischen Ausrichtung berücksichtigen sollten, wenn die Netzabdeckung und Infrastrukturversorgung in vielen Teilen Deutschlands noch mangelhaft sind.

2. Bei der Befragung hat sich ebenfalls herausgestellt, dass Frauen als IT-Dienstleister oder als dafür Verantwortliche in KMU, kaum vertreten waren. Gegebenenfalls sollte dieser Punkt unter Betrachtung des Fachkräftemangels in der Branche und möglicher Incentivierungen genauer betrachtet werden.

Aus der Frage hinsichtlich der **Zusammenarbeit mit IT-Dienstleistern** hat sich ergeben, dass kleine KMU Schwierigkeiten haben, Anbieter für ihre ausgeschriebenen IT-Leistungen zu finden. Für die Bereitstellung dieser IT-Dienstleistungen wird oftmals auf die Hilfe aus der Nachbarschaft und dem Bekanntschafts-/Freundschaftskreis zurückgegriffen. Zumindest stellen regionale Nähe und Nachbarschaft laut dieser Aussagen bei der Auswahl der IT-Dienstleistung wichtige Faktoren dar. Angebotene Branchenlösungen werden als Schritt in die richtige Richtung erachtet, sind aber insbesondere unter den persönlichen IT-Dienstleistern der KMU umstritten. Dies könnte womöglich damit zusammenhängen, dass einige IT-Dienstleistungen sich nicht nach Branchenspezifikationen aufteilen lassen, wie es sich manche fachfremde Personen vielleicht vorstellen. Es wird von den KMU, statt einer One-fits-all Lösung, eine individuelle Behandlung gefordert. Für die Umsetzung einer passenden IT bzw. IT-Sicherheitslösung stellt sich die Rolle der Geschäftsführung, internen SystemadministratorInnen oder eines/r IT-Beauftragten als viel entscheidender heraus. Demnach würde die Aufstellung des Unternehmens hinsichtlich der IT-Sicherheit von der thematischen Motivation und dem Beschäftigungsgrad dieser Person abhängig sein.

In Bezug auf das IT-Budget können aus den Befragungen nur Schätzwerte abgeleitet werden. Es wurden Prozentsätze von ungefähr 5% des Umsatzes bis zuweilen auf 20% angegeben.

Der **Fachkräftemangel** und die Auslagerung der IT-Dienstleistungen an Dritte werden der Beschreibung nach, durch Eigenarbeit und „Reinwurschteln“ unter den kleinsten und kleinen Unternehmen überwunden. Aus diesem Umstand und der Tatsache, dass sich kaum externe BetreuerInnen für kleine Projekte finden lassen, ergeben sich insgesamt weniger Projekte für die befragten KMU. Es zeigt sich, dass insbesondere Klein(st)unternehmen mit viel Tagesgeschäft und geringer Nutzung digitaler Anwendungen eine mangelhafte IT-Sicherheit aufweisen. Auch geht aus den Aussagen hervor, dass speziell Apple-NutzerInnen dieser Gefahr ausgesetzt sind, weil Apple-Software als vermeintlich sicher unter ihnen gilt.

9.2. Studienergebnisse der quantitativen Befragung der KMU

Nachfolgend werden die wesentlichen Ergebnisse der quantitativen KMU-Befragung in den Kategorien

- Statistische Daten der Unternehmen,
- Informationsbeschaffung zu IT-Sicherheit,
- Regelungen und Prozesse,
- Zuständigkeiten im Unternehmen,
- Wahrgenommene Risiken der IT-Sicherheit,
- Besondere Hemmnisse,
- Öffentliche Förderung und
- Zusammenarbeit mit IT-Dienstleistern zusammengefasst.

9.2.1. Statistische Daten der Unternehmen

An der Umfrage nahmen insgesamt 176 Unternehmen teil. 89 Fragebögen wurden vollständig ausgefüllt. Sie sind die Grundlage der folgenden Analyse. Die Umfrage hat sich ausschließlich an KMU gerichtet. Sofern nicht anders angegeben, wurde auf die Darstellung der unbeantworteten Fragen in den nachfolgenden Grafiken verzichtet. Nur 2% gaben an mehr als 500 MitarbeiterInnen zu beschäftigen. Den größten Anteil der Befragten machen Kleinstunternehmen mit bis zu 9 MitarbeiterInnen (41%) aus. 24% der Unternehmen haben zwischen 10 und 49 Beschäftigte. Weitere 15% der Unternehmen sind dem Bereich mittelgroße KMU mit 50 bis 499 MitarbeiterInnen zuzuordnen.

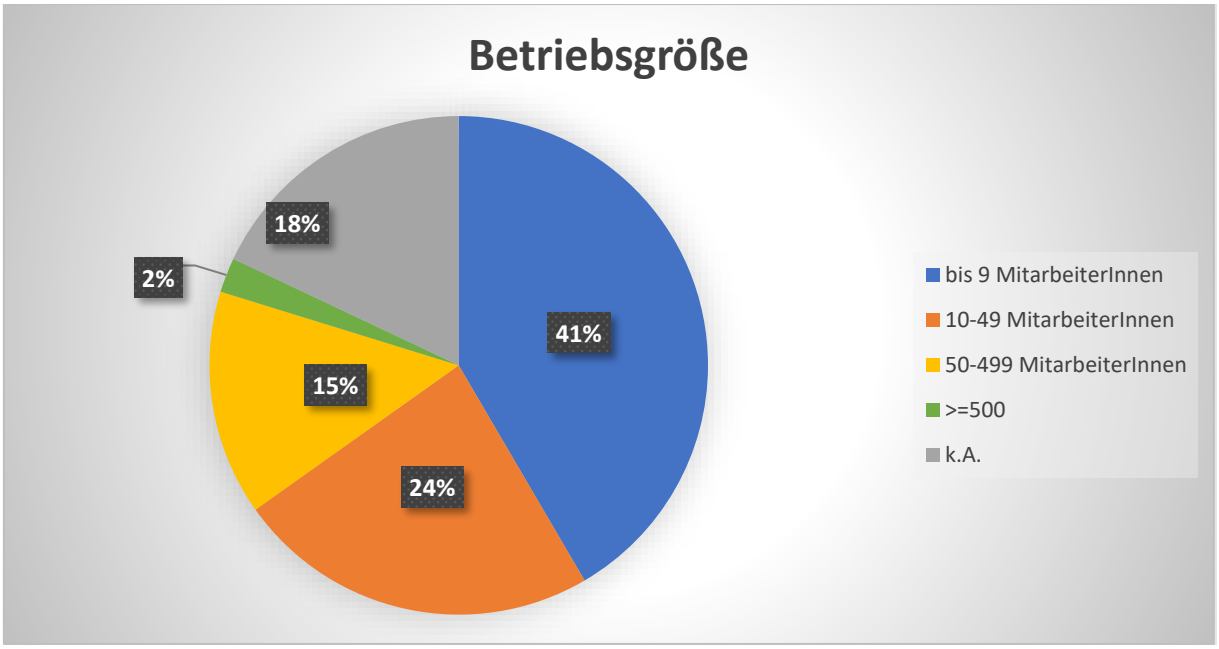

Abbildung 42 – Größe des Unternehmens (Anzahl MitarbeiterInnen in Vollzeitäquivalente).

Die meisten an der Umfrage beteiligten Unternehmen kommen aus Bayern (17%), Berlin (15%), gefolgt von Niedersachsen (7%) sowie Nordrhein-Westfalen (6%). 24% der Unternehmen gaben keine Angaben über den Sitz ihres Unternehmens an. Insgesamt haben mit 48% mehr Unternehmen aus den „alten“, als aus den „neuen“ Bundesländern (inklusive Berlin) mit 28% an der Umfrage teilgenommen. Die restlichen 24% haben keine Angabe zum Sitz des Unternehmens gemacht. Damit ergibt sich proportional betrachtet auf die Anzahl der vorhandenen KMU in Deutschland eine Übergewichtung derjenigen KMU, die ihren Sitz in den neuen Bundesländern haben.

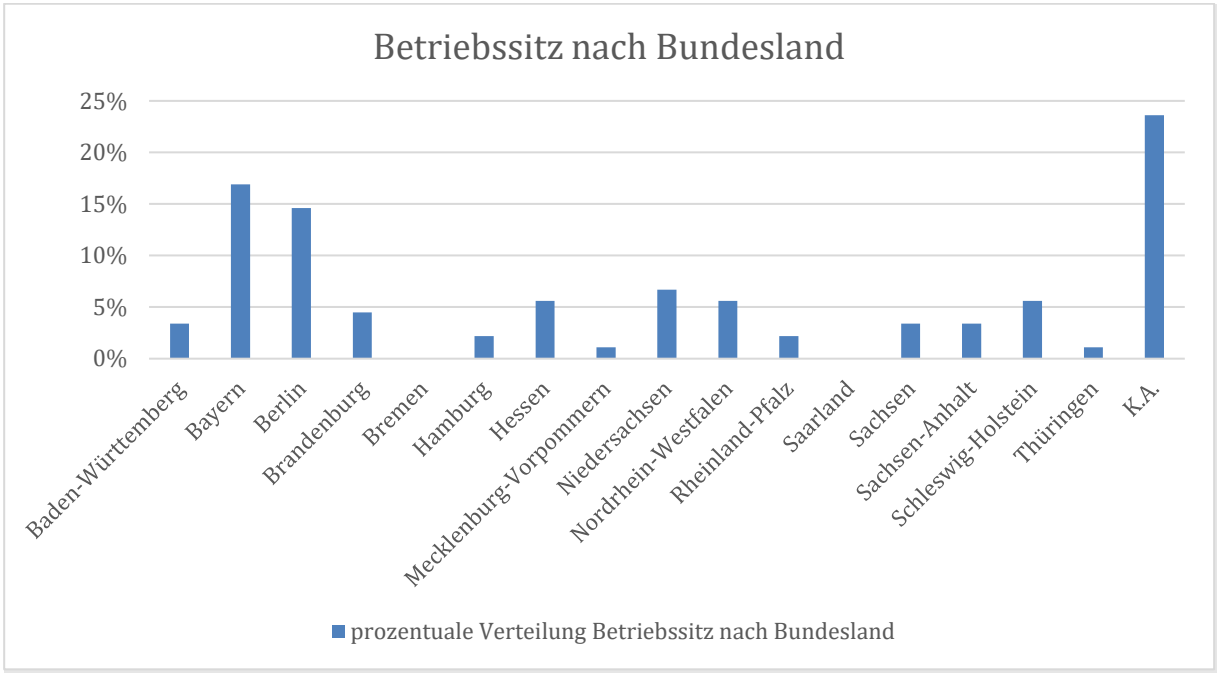

Abbildung 43 – Verteilung nach Hauptbetriebssitz der an der Umfrage beteiligten KMU.

35% der befragten Unternehmen sind regional, 20% deutschlandweit, 15% in der DACH Region bzw. in der EU und 16% international tätig. Die auswärtige Marktbearbeitung von ungefähr 31% (D-A-CH, EU und international) im Vergleich zur heimischen von 55% (regional, deutschlandweit), lässt eine ausgeprägte Diversifizierungsstrategie hinsichtlich der Zielmärkte der befragten KMU vermuten. Nach welchen Kriterien die Marktbearbeitung tatsächlich vorgenommen wurde, ob das Unternehmen bewusst oder notgedrungen regional oder national operiert oder sich in der Konsolidierungs- oder Expansionsphase befindet, lässt sich aber aus den Antworten nicht abschließend ableiten.

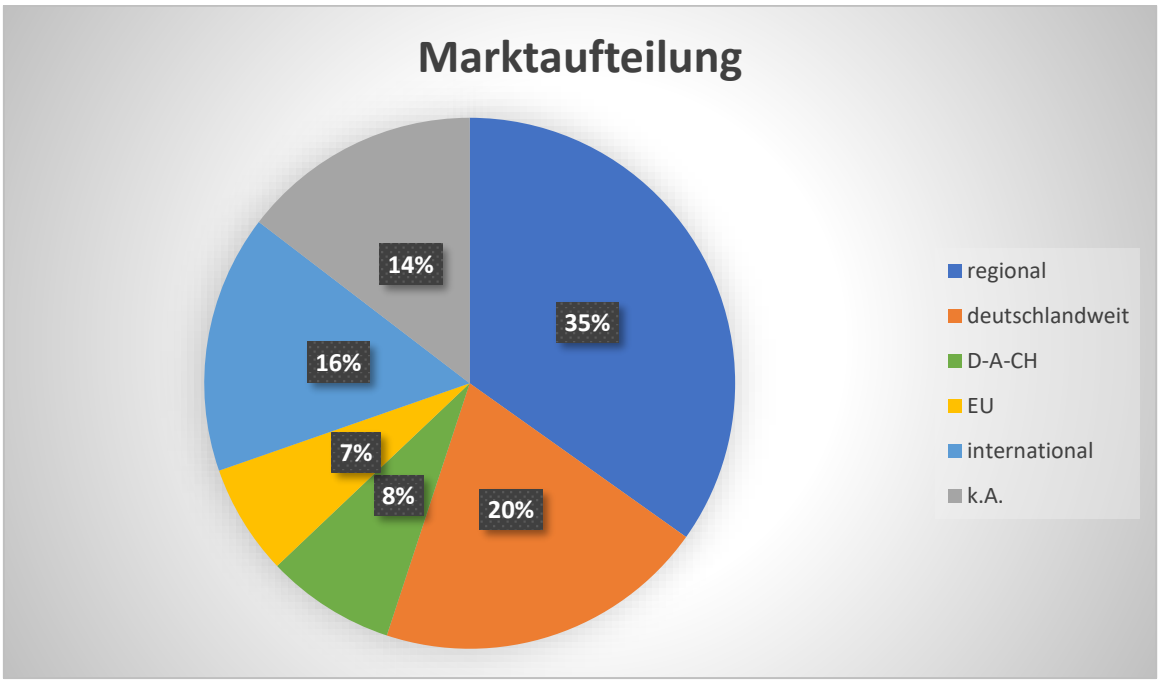

Abbildung 44 – Marktaufteilung der befragten KMU.

KMU aus den unternehmensnahen Dienstleistungssektor (39%) stellen bei dieser Umfrage die am stärksten vertretenen dar. Gefolgt werden diese von Unternehmen aus dem Baugewerbe (17%), Verkehr, Information und Kommunikation (13%), sowie Handel (12%) und verarbeitendem Gewerbe (10%). Unternehmen aus dem Bergbau, Energie-, Wasserversorgung und Entsorgungsbranche haben an dieser Umfrage nicht teilgenommen. Die Unterrepräsentation dieser Branche ist dem Umstand geschuldet, dass es kaum mittelständische und inhabergeführte Unternehmen aus diesem Sektor gibt. KMU aus den personenbezogenen bzw. Finanz-Versicherungsdienstleistungen und Wohnungswesen, machen insgesamt (10%) aus.

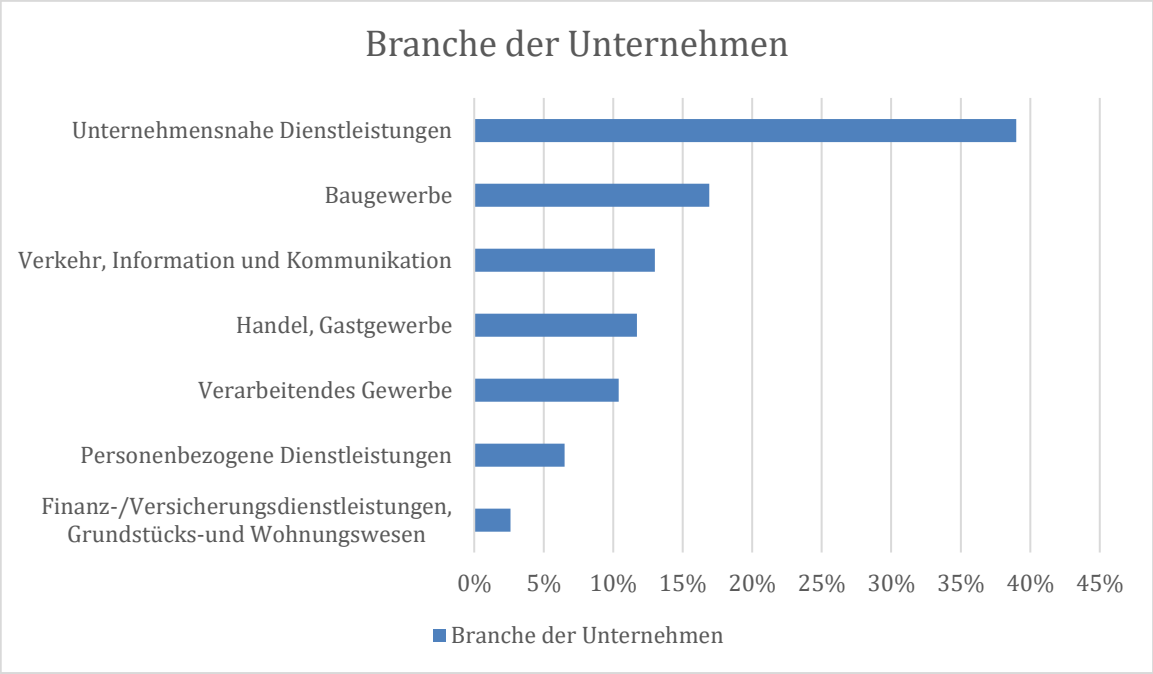

Abbildung 45 – Branchen in denen die befragten KMU tätig sind.[155]

In Bezug auf die Fragen, wie sich ihr Unternehmen vor der Covid-19 Pandemie entwickelt hat bzw. sich danach entwickeln wird, haben sich bei der Einschätzung der befragten KMU deutliche Veränderungen ergeben. Während vor dem weltweiten Ausbruch des Virus und dem einhergehenden Wirtschaftseinbruch 70% der KMU angaben, dass ihr Unternehmen wächst, gehen inzwischen nur noch 48% von einem weiteren Wachstum in nächster Zeit aus. Folglich stieg der Anteil der KMU, die für die kommende Zeit eine stagnierende Entwicklung ihres Unternehmens prognostizieren, von 24% auf 44%. Vergleichsweise moderat fällt hingegen der gesteigerte Anteil der Antworten von KMU aus, die für ihr Unternehmen ein schrumpfendes Entwicklungsumfeld von 6% auf 8% sehen. Nichtsdestotrotz lassen diese Angaben ein für das Ausmaß der Krise vergleichsweise optimistisches Entwicklungsszenario, zumindest für die an dieser Umfrage teilnehmenden KMU, zu.

[155] Unternehmen aus dem Bergbau, Energie-, Wasserversorgung, Entsorgung haben keine Angaben gemacht.

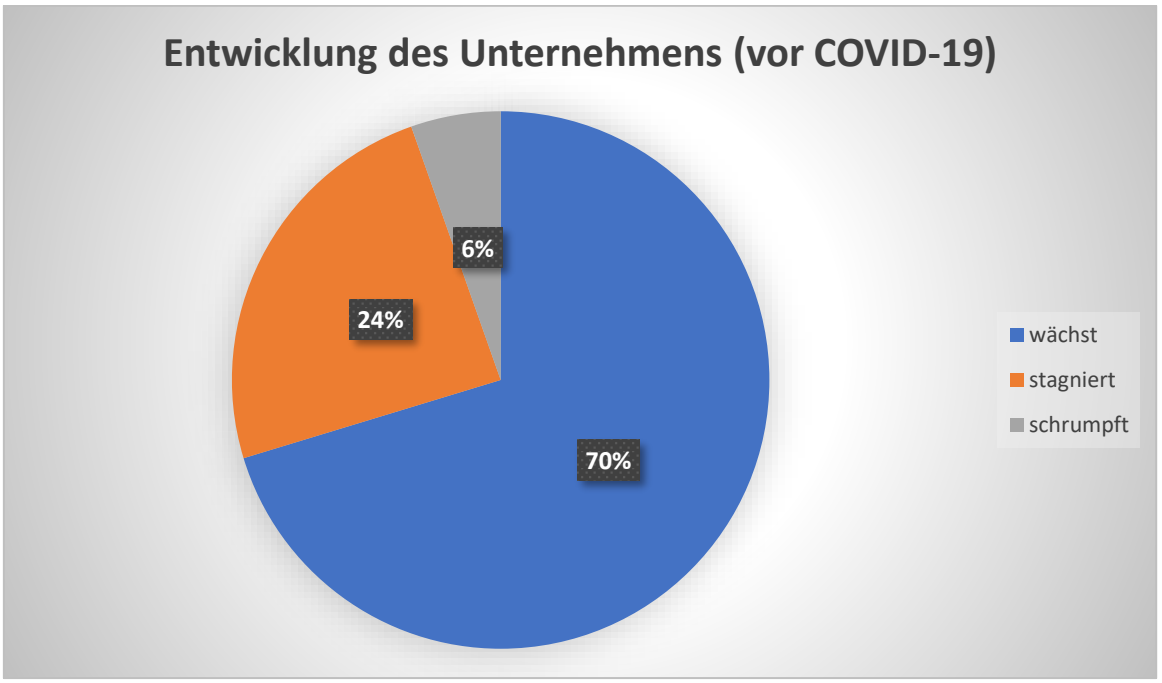

Abbildung 46 – Entwicklung des Unternehmens (vor Covid-19-Krise).

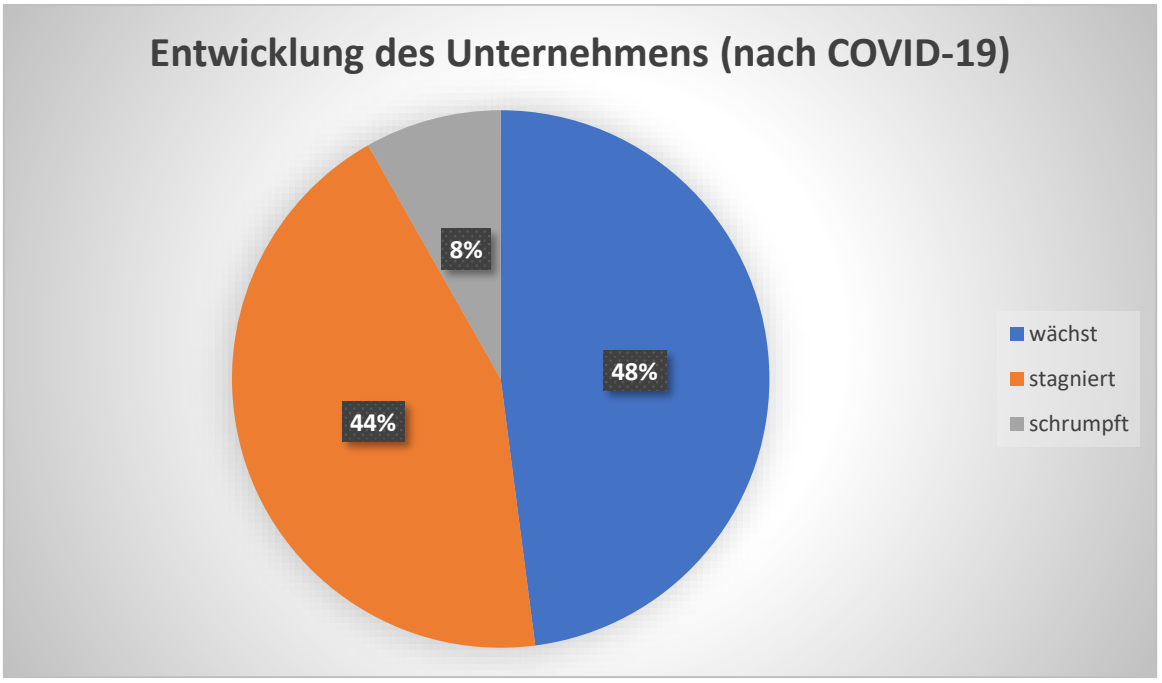

Abbildung 47 – Entwicklung des Unternehmens (nach Covid-19-Krise).

Der überwiegende Teil der an der Umfrage teilnehmenden KMU gab an, entweder die Rechtsform einer Gesellschaft mit beschränkter Haftung (GmbH) mit 45% oder den eines Einzelunternehmens (29%) einzunehmen. Die weiteren

Unternehmen gaben an, eine GmbH Co. KG (13%), eine Gesellschaft bürgerlichen Rechts (GbR) mit 5% oder eine Aktiengesellschaft (AG) mit 3% zu sein. Weitere Unternehmensrechtsformen, wie offene Handelsgesellschaften (OHG) oder Kommanditgesellschaften (KG) werden unter Sonstige zusammengefasst.

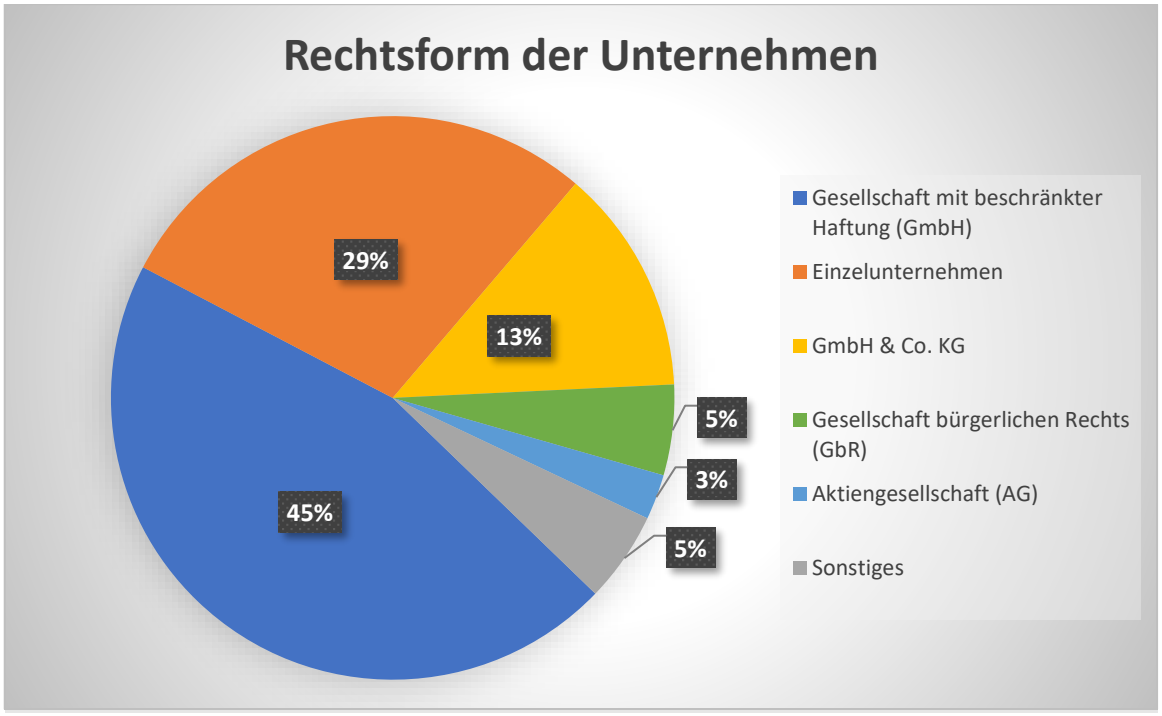

Abbildung 48 – Rechtsform der Unternehmen.

Hinsichtlich der Frage, durch wen sich KMU bei der Durchsetzung ihrer Interessen vertreten lassen, kam bei den teilnehmenden Unternehmen dieser Umfrage heraus, dass sie sich durch eine Vielzahl verschiedener Verbände vertreten lassen. Unter den meist genannten zählen die Handwerkskammern (11%), diverse Innungen (8%) oder die regionalen Industrie- und Handelskammern (4%). Mehrfach und als einziger nennenswerter Verband in dieser Umfrage, wurde der Bundesverband mittelständische Wirtschaft Unternehmerverband Deutschland e.V. (BVMW) mit 7% genannt. Alle weiteren zwei- oder einfach aufgezählten Verbände und Vereine wurden der Übersicht halber unter Verschiedene (28%) zusammengefasst. Als solche stellen sie die größte Gruppe dar und zeigen die heterogene Organisationsstruktur innerhalb der teilnehmenden KMU auf. Der größte Anteil der befragten Unternehmen (40%) nannte keine Verbände, durch die sie sich bei der Durchsetzung ihrer Interessen vertreten fühlen.

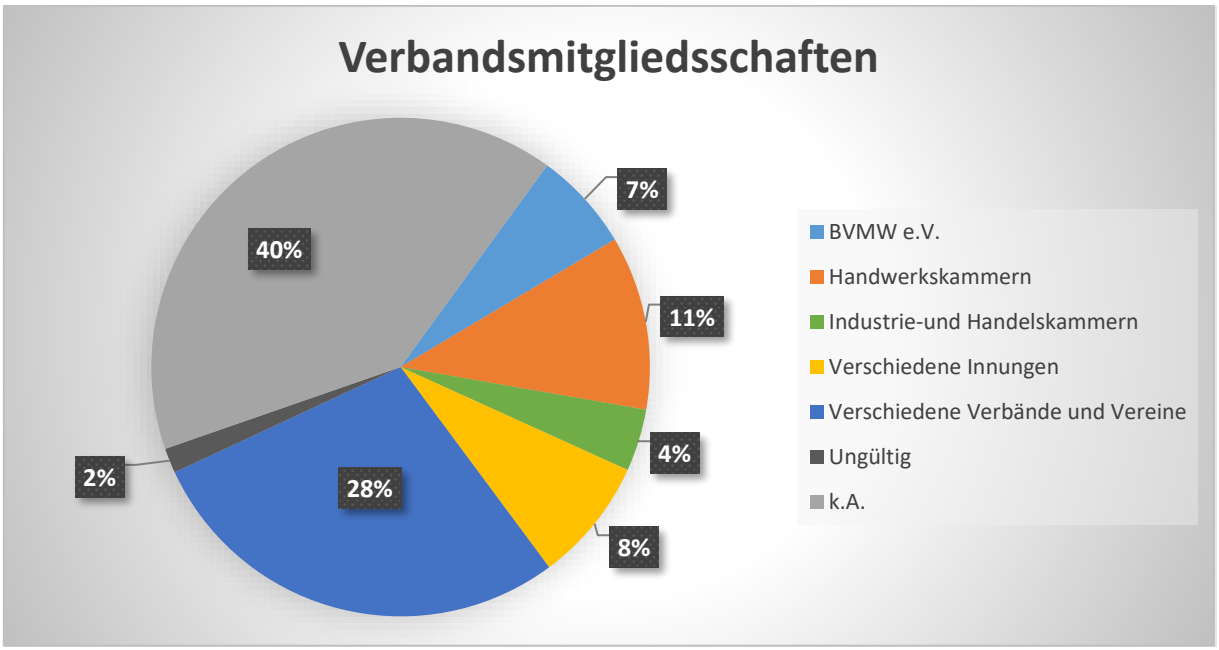

Abbildung 49 – Wichtige Verbände für KMU.

Als die KMU danach befragt wurden, ob sie eine/n externe/n Datenschutzbeauftragte/n für ihr Unternehmen hinzuziehen, hat sich unter den Unternehmensangaben eine eindeutige Tendenz abgezeichnet. Gerade einmal 21% der UmfrageteilnehmerInnen bejahen die Inanspruchnahme einer solchen externen Dienstleistung. Die Frage gibt aber keine Rückschlüsse darauf, ob nicht diese Rolle von einem/r internen MitarbeiterIn in diesem Unternehmen wahrgenommen wird. Aufgrund der Vielzahl an Kleinstunternehmen bei der Beantwortung dieser Umfrage, muss jedoch davon ausgegangen werden, dass diese Kompetenz von einer Person aus der Belegschaft nur zum Teil oder im Unternehmen erst gar nicht wahrgenommen wird.

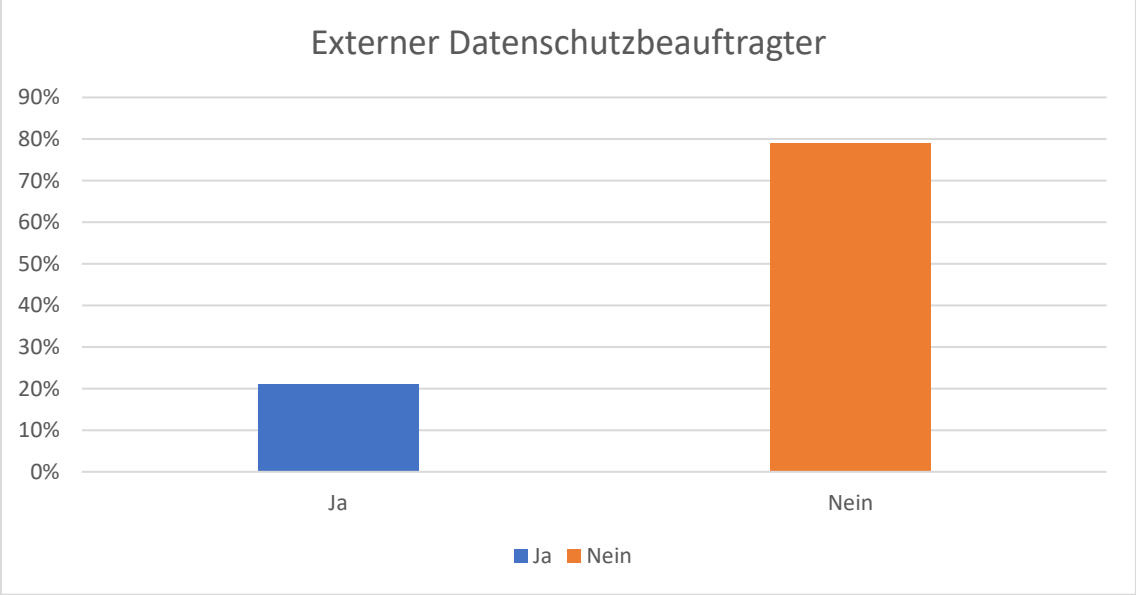

Abbildung 50 – Externer Datenschutzbeauftragter im Unternehmen.

Ferner sollten die befragten Unternehmen Angaben zu dem finanziellen Aufwand machen, der intern für die IT-Sicherheit betrieben wird. Hierzu konnten die Unternehmen den prozentualen Anteil vom IT-Budget bestimmen, der von IT-Sicherheit eingenommen wird. Aus den gemachten Angaben geht hervor, dass knapp die Hälfte der KMU (49%) zwischen 1 und 10% ihrer IT-Ausgaben speziell für ihre IT-Sicherheit aufwenden. Die nächstgrößere Gruppe (24%) gab an 11 bis 20% für diese Aufgabe aufzuwenden. Weitere KMU (11%) gaben zu erkennen, dass sie zwischen 21 und 30% ihres IT-Budgets für die Sicherung ihrer IT veranschlagen. Überdurchschnittlich hohe Ausgaben verzeichneten hingegen nur eine geringe Anzahl KMU (11%), die zwischen 31 und 70% ihres IT-Budgets für IT-Sicherheit reservieren. Einige wenige Unternehmen (4%) gaben sogar an, über keine Ausgaben in diesem Bereich zu haben oder zumindest keine konkrete Prozentzahl nennen zu können.

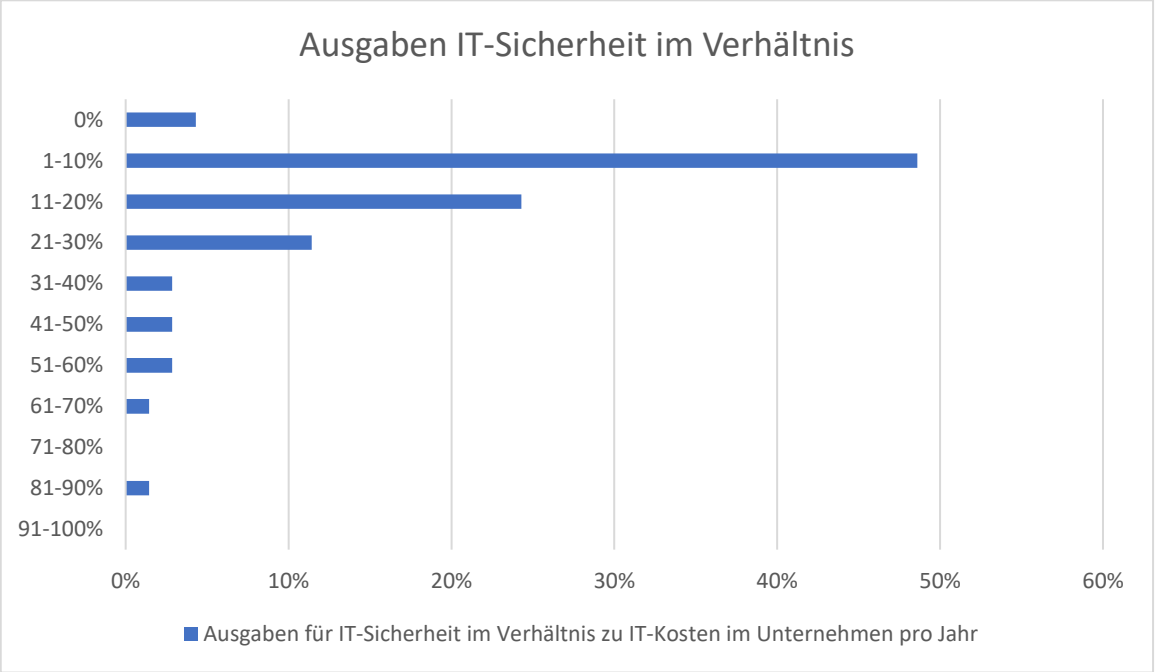

Abbildung 51 – Anteil der Ausgaben für IT-Sicherheit im Verhältnis zum IT-Budget der KMU.

In der nachfolgenden Frage sollte von den KMU Auskunft darüber gegeben werden, wie hoch der prozentuale Anteil der Ausgaben des IT-Budgets ist, der für externe IT-Dienstleistungen eingesetzt wird. In diesem Falle zeigt sich, aufgrund der Verteilung der Angaben durch die KMU, ein differenzierteres Bild. Während über drei Viertel der KMU (76%) die Kosten für die Inanspruchnahme auf 1 bis 30% taxieren, geben 14% an, zwischen 71 und 100% ihres zur Verfügung stehenden IT-Budgets für auswärtige Dienstleister vorzusehen. Ein weiterer Teil der befragten KMU (8%) gab an, zwischen denen zu liegen, die proportional viel für externe IT-Services zu verwenden und denen, die relativ wenig für diesen Kostenfaktor vorsehen. Der überwiegende Teil der befragten KMU scheinen entweder auf ihre eigenen Fähigkeiten zu setzen oder die wahrscheinlich hohen Kosten für die Heranziehung auswärtiger IT-Services zu scheuen. Letzteres kann man aus den Antworten zu dieser Frage nicht herleiten, sondern nur vermuten.

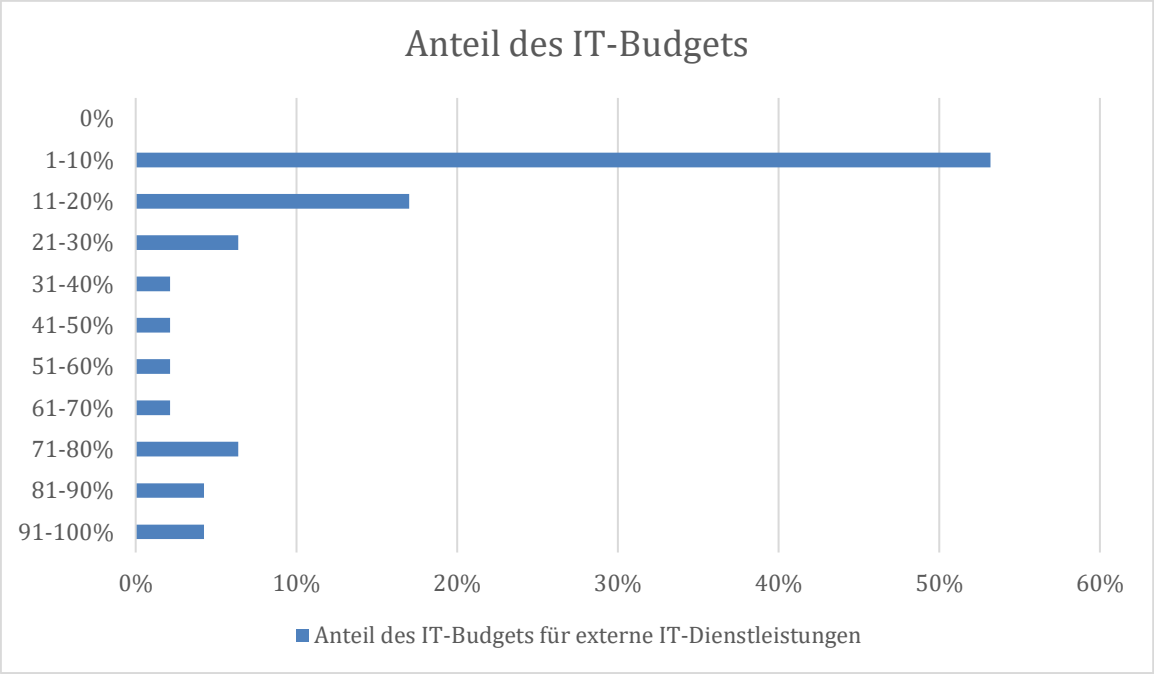

Abbildung 52 – Anteil der Ausgaben für externe IT-Dienstleister im Verhältnis zum IT-Budget der KMU.

Das Vorhandensein spezieller IT-Sicherheitsbudgets in der Jahres-Budgetplanung wurden bei der nachfolgenden Frage von den KMU überwiegend (81%) verneint. 7% gaben an über Budgets zu verfügen, die im Falle von IT-Notfällen bereitgestellt werden oder die für präventive Maßnahmen aufgewandt werden können. Auch wenn der Anteil sehr niedrig ist, kann nicht daraus gefolgert werden, dass von Seiten der KMU kein Interesse an dem Aufbau dieser IT-Sicherheitsmittel besteht.

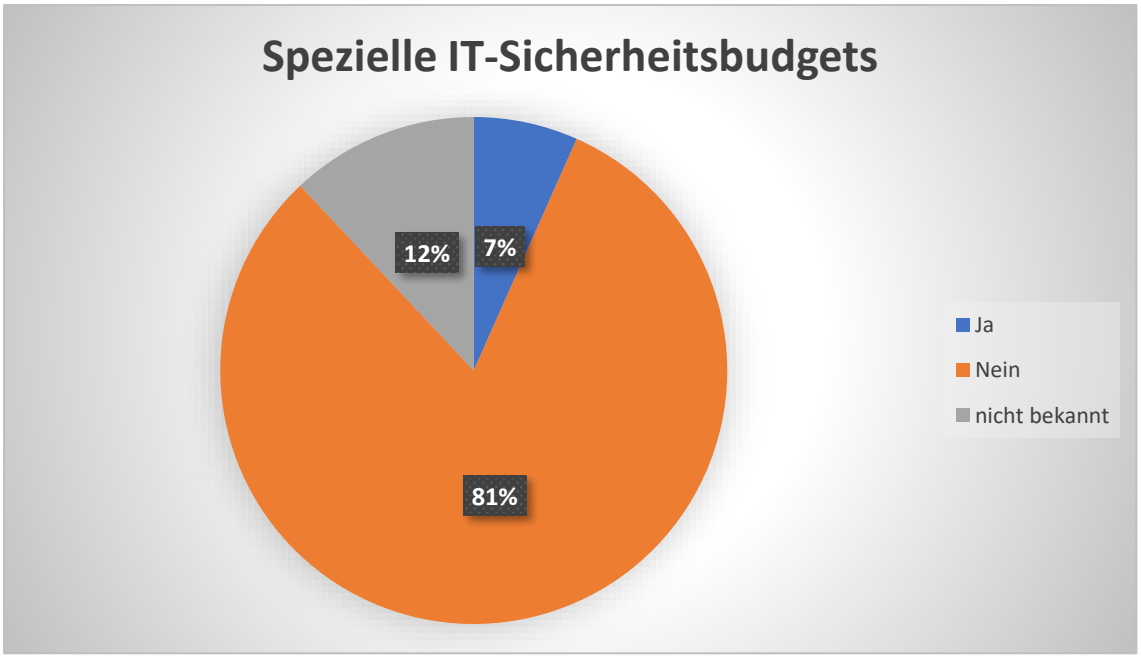

Abbildung 53 – Spezielle IT-Sicherheitsbudgets in der Jahres-Budgetplanung der KMU.

9.2.2. Informationsbeschaffung zu IT-Sicherheit

Zu der Frage wie sich KMU über Angriffe und IT-Sicherheitsrisiken informieren, konnten mehrere Antworten gegeben und nach einer Rangfolge kategorisiert werden. Aus der Vielzahl an Antwortmöglichkeiten ergab sich, dass sich KMU zu einem großen Teil über die klassischen Kanäle Tagespresse/TV-Nachrichten (60%) und Fachzeitschriften inklusive online Reports (48%) informiert. Als weitere wichtige Informationsquellen werden Kammern (42%), IHK oder HWK, genannt. Ferner informiert sich ein Teil der Unternehmen in nennenswerter Weise über ihren IT-Dienstleister (36%), Bundesbehörden (33%) und Social-Media-Kanäle (34%) oder Fachzeitschriften einschließlich gedruckter Reports (27%). Es sei noch zu erwähnen, dass sich ein nicht unerheblicher Teil der TeilnehmerInnen über Bekannte (23%) zu dieser Thematik informiert hält. Die Informationsbeschaffung im Hinblick auf die IT-Sicherheit kann als heterogener Prozess beschrieben werden, da viele unterschiedliche Medienkanäle zu einem unterschiedlich hohen Grad herangezogen werden.

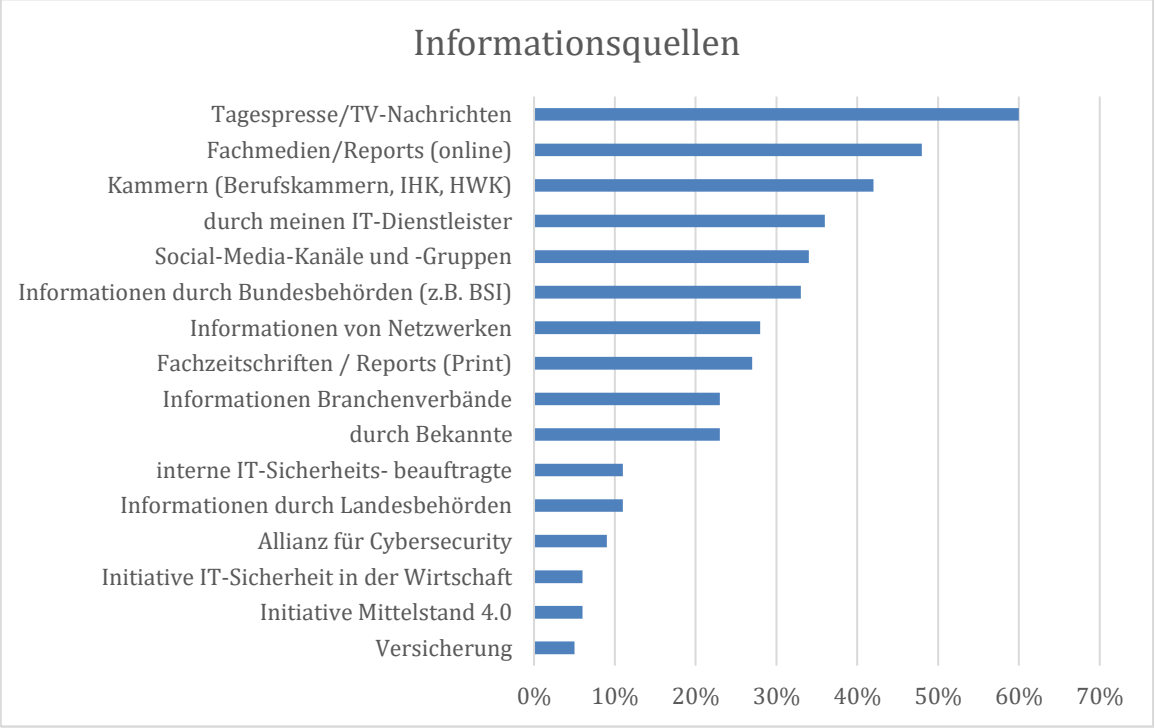

Abbildung 54 – Informationsquellen der KMU zu Angriffen und IT-Sicherheitsrisiken.

Mehr als die Hälfte (56%) der TeilnehmerInnen der Umfrage geben an, sich auf kontinuierlicher Basis mit der IT-Sicherheit ihres Unternehmens zu befassen. Ein Drittel (33%) der KMU gab wiederum an, sich nur bei Bedarf, u.a. im Falle von Angriffen oder anderen Problemen, mit dieser IT-Sicherheitsthemen auseinanderzusetzen. Weitere Befragte gaben an, sich nur über längere Zeiträume verteilt mit der IT-Sicherheit zu beschäftigen. Demnach beschäftigen sich 5% der antwortenden Unternehmen monatlich, 4% quartalsweise und weitere 2% halb- oder jährlich mit der Sicherheit der IT in ihrem Unternehmen. Zusammengerechnet stellen die KMU, die sich nicht ausreichend mit dem Schutz

ihres Unternehmens befassen, fast die Hälfte (44%) der Befragten dar. Dieser Umstand kann als ein ernstzunehmendes Risiko für die Geschäftsmodelle der KMU bezeichnet werden.

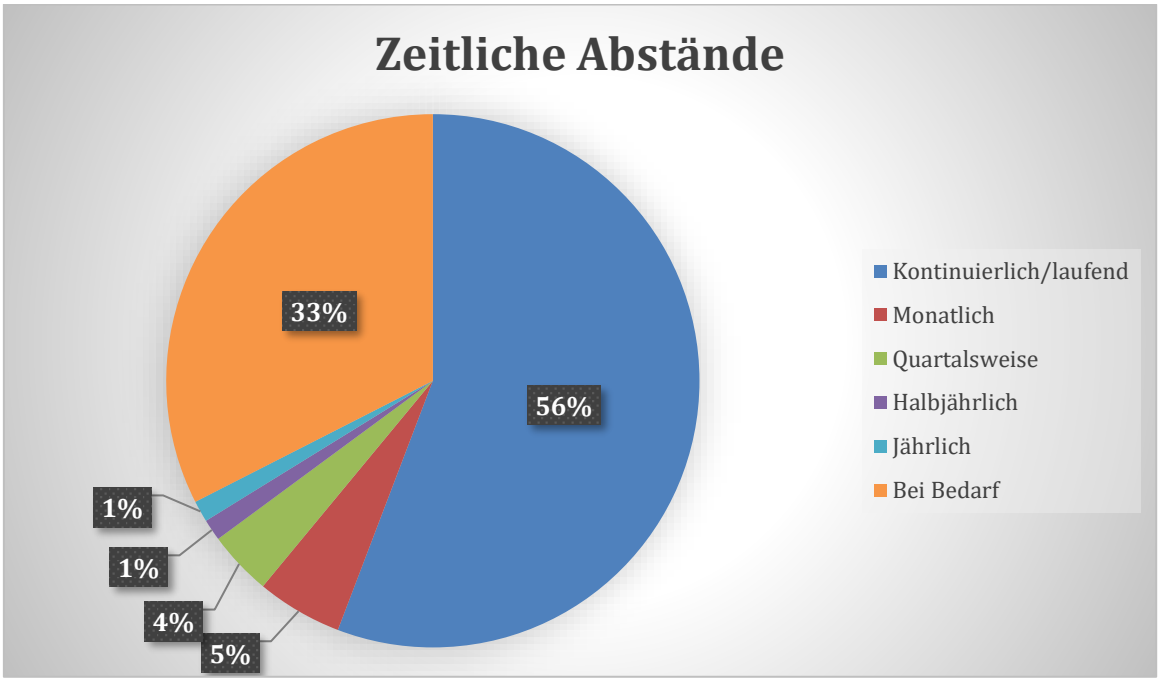

Abbildung 55 – Zeitliche Abstände in denen sich KMU mit IT-Sicherheit befassen.

9.2.3. Regelungen und Prozesse

Zu den ausgewählten Regelungen und Prozessen innerhalb der KMU hatten die TeilnehmerInnen die Möglichkeit, aus acht Verfahrensoptionen zu wählen und auch Mehrfachnennungen anzugeben. Es wird dabei deutlich, dass nur eine geringe Anzahl über ein vollwertiges Informationssicherheitsmanagementsystem (16%) verfügt. Gefolgt wird diese Auswahl von IT-Sicherheits-Leitlinien (30%). Zur Vorbereitung auf IT-Sicherheitsprobleme greift die überwiegende Mehrzahl von 43% der KMU auf vorbereitete IT-Sicherheitskonzepte zurück. Bei 30% der KMU treten bei Vorfällen IT-Notfallregelungen in Kraft bzw. sind diese geplant. Technische Richtlinien werden von 19% der befragten genannt. Weitere KMU (37%) verfügen zumindest über Verfahrensanweisungen, die beim Eintreten eines Angriffs gelten. 2% gaben an, dass sie weiteren Regelungen folgen würden. Fast 16% der Befragten geben an über keinerlei Regelung oder Prozesse hinsichtlich der IT-Sicherheit zu verfügen. Der hohe Anteil der KMU, der keinerlei oder nur unzureichende IT-Sicherheitsvorkehrungen vorweist, deutet entweder auf eine mögliche Unterschätzung der Gefahren seitens der KMU hin oder sie werden bewusst, aufgrund mangelnder Ressourcen, Kenntnisse und Mittel in Kauf genommen. Ferner ist davon auszugehen, dass ein nicht unerheblicher Teil der TeilnehmerInnen ihre IT-Sicherheitslage höher einschätzt, als sie tatsächlich ist.

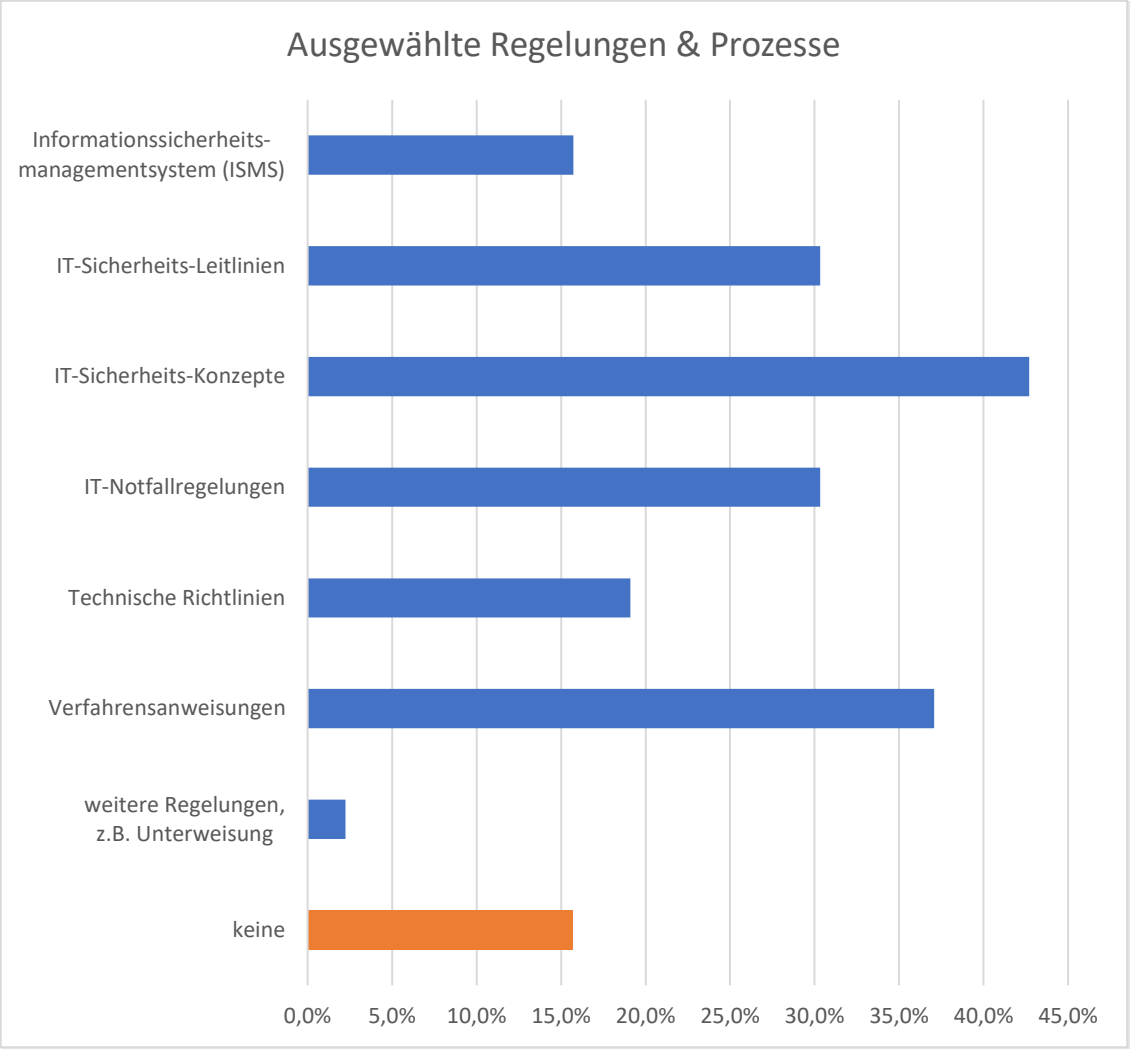

Abbildung 56 – Regelungen und Prozesse zu IT-Sicherheit der KMU.

9.2.4. Zuständigkeiten im Unternehmen

Die Verantwortung über die IT-Sicherheit obliegt in den meisten Fällen der Geschäftsführung (45%). Erst mit einem deutlich geringeren Anteil folgt die eigene IT-Abteilung (15%) als Antwortmöglichkeit unter den KMU. In weiteren Fällen befasst sich hauptsächlich ein/e zuständige/r MitarbeiterIn (12%) oder der externe Dienstleister (11%) mit dem IT-Schutz im Unternehmen. Mit jeweils 5% gaben die KMU an, einen Verantwortlichen nur bei Bedarf zu ernennen oder eine/n externe/n SystemadministratorIn bzw. FreelancerIn zur Verfügung zu haben. Die Beauftragten für Informationssicherheit (4%) und Datenschutz (3%) wurden am seltensten genannt. Der hohe Anteil der Zuständigkeit für IT-Sicherheit in den Händen der Geschäftsführung könnte zu zweierlei Rückschlüssen führen. Zum einen, dass sie von hoher Priorität und Wichtigkeit für die Funktionsweise der Unternehmung ist und daher auf Ebene der Geschäftsführung verantwortet werden muss. Zum anderen, weil sonst kein/e MitarbeiterIn, aufgrund der Größe des Unternehmens, diese Aufgabe erfüllen könnte. Unter den Teilnehmenden der Umfrage besteht, wie sich am Anfang der Auswertung ergeben hat, ein großer Prozentsatz aus Kleinstunternehmen.

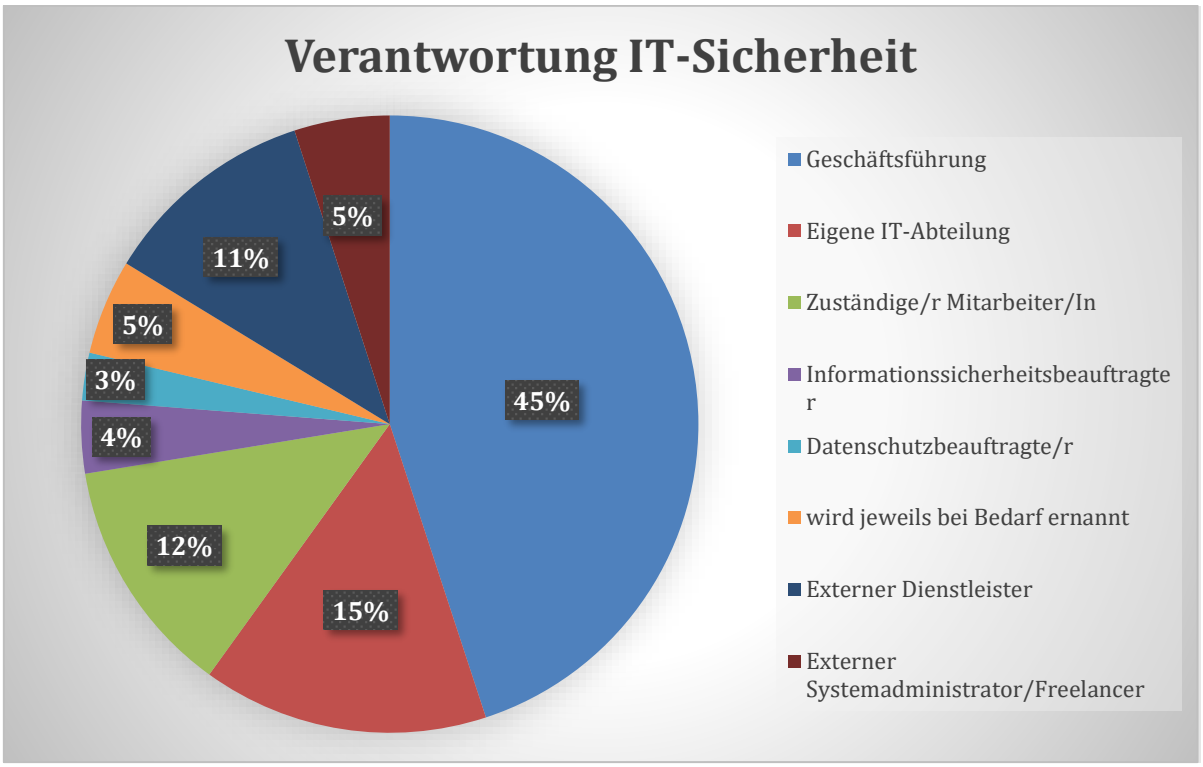

Abbildung 57 – Zuständigkeit über IT-Sicherheit der KMU.

9.2.5. Wahrgenommene Risiken der IT-Sicherheit

Wie im Falle der Befragung der IT-Dienstleister, wurden die teilnehmenden KMU nach ihrer Einschätzung bzgl. der Eintrittswahrscheinlichkeit von Bedrohungen in den Bereichen des menschlichen Versagens (z. B. mangelnde IT-Kenntnisse im Zusammenhang mit Angriffen, Schadsoftware und Phishing), technischen Versagens (z. B. unzureichender Schutz der IT-Infrastrukturen), Organisationsversagens (z. B. ungenügende Regelungen zu Zugangsmanagement oder Sicherheit von Identitäten) und von Angriffen (z.B. Schadsoftware, Spoofing, Identitätsdiebstahl, Botnetze DDoS-Attacken, Phishing, Ransomware) befragt.

Die **Faktoren Mensch und Angriffe** werden laut TeilnehmerInnen **als die größeren potenziellen Risiken für die IT-Sicherheit von KMU** angesehen. So schätzen 12% die Eintrittswahrscheinlichkeit von menschlichem Versagen als *sehr hoch* und weitere 19% als *eher hoch* ein. Angriffe werden mit 7% als sehr hohes bzw. mit 21% als eher hohes Risiko bei der Eintrittswahrscheinlichkeit von Bedrohungen eingeschätzt. Durch technisches Versagen, Opfer eines Cyber-Vorfalls zu werden, gaben gerade einmal 1% als *sehr hohes* und lediglich 12% der Befragten als *eher hohes* Risiko an. Im Bereich Organisationsversagen war kein KMU der Meinung, dass durch z.B. mangelnde oder unzureichende interne Prozesse ein *sehr hohes* Risiko besteht. Hier gaben zumindest 20% an, ein *eher hohes* Risiko in diesem Faktor zu erkennen.

Im direkten Vergleich der Antwortmöglichkeiten *sehr hoch* und *eher hoch* mit den anderen Bereichen zeigt sich, dass die KMU die Eintrittswahrscheinlichkeit von menschlichem Versagen am höchsten bewerten. Es folgen Angriffe, Organisationsversagen und zuletzt technisches Versagen.

Die getroffenen Aussagen der KMU könnten einen Hinweis dafür liefern, dass die externen Risiken, wie sie sich durch Schadsoftware, Phishing etc. ergeben, überproportional hoch eingeschätzt werden. Während interne Faktoren, wie insbesondere menschliches oder Organisationsversagen, vergleichsweise niedrig angesetzt werden. Zwar wurde menschliches Versagen als Hauptfaktor genannt, dennoch könnte sich diese Einschätzung insgesamt betrachtet nur auf einem moderaten Niveau bewegen. Dies wäre dann der Fall, wenn man sich die tatsächliche Häufigkeit der IT-Schäden vor Augen führt, die durch menschliches Versagen verursacht wird.

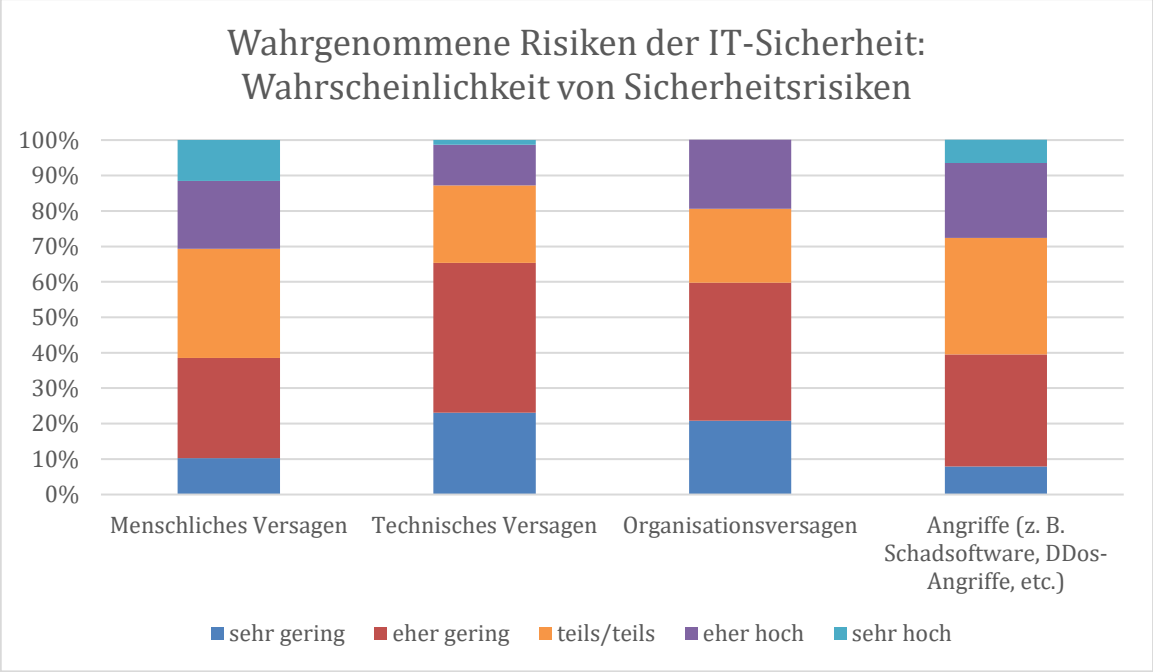

Abbildung 58 – Bewertung der Eintrittswahrscheinlichkeiten für die jeweiligen Bedrohungen aus Sicht der KMU.

In der folgenden Grafik sind im Vergleich die Antworten der KMU zusammengefasst, die ein *sehr hohes* und *eher hohes* Risiko für menschliches und technisches Versagen, Organisationsversagen sowie für Angriffe bei ihren KMU-Kunden sehen.

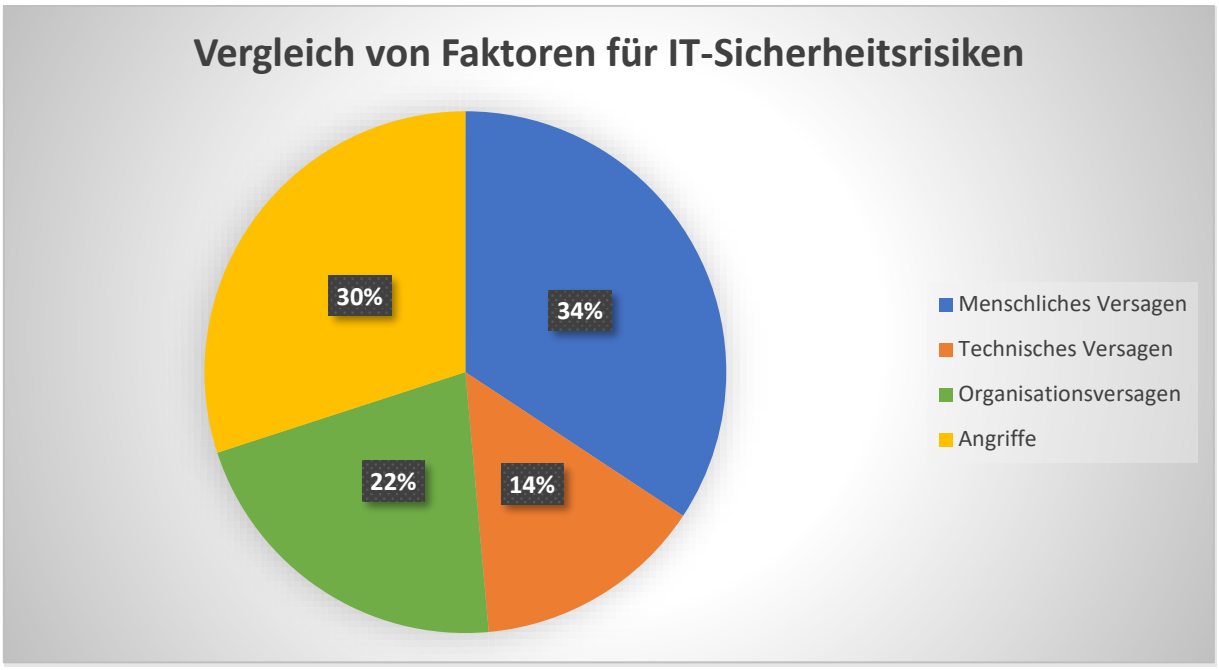

Abbildung 59 – Im Vergleich die Eintrittswahrscheinlichkeiten eher hoch und sehr hoch für die jeweiligen Bedrohungen aus Sicht der KMU.

Die **Faktoren Angriffe und Mensch** werden laut TeilnehmerInnen am ehesten für tatsächlich eintretende Schäden verantwortlich gemacht. So geben 19% an, dass Angriffe zu einem *sehr großen* und weitere 29% zu einem *eher großen* Maß für entstandenen Schäden aufkommen. Menschliches Versagen wird mit 15% als *sehr große* bzw. mit 22% als *eher große* Schadensursache angegeben. Durch technisches Versagen, einen Schadensfall zu erleben, geben lediglich 9% als *sehr große* und 21% der Befragten als *eher große* Ursache an. Was den Faktor Organisationsversagen anbetrifft, waren nur 7% der KMU der Meinung, dass dadurch *sehr große* und, weitere 18% *eher große* Schäden entstehen.

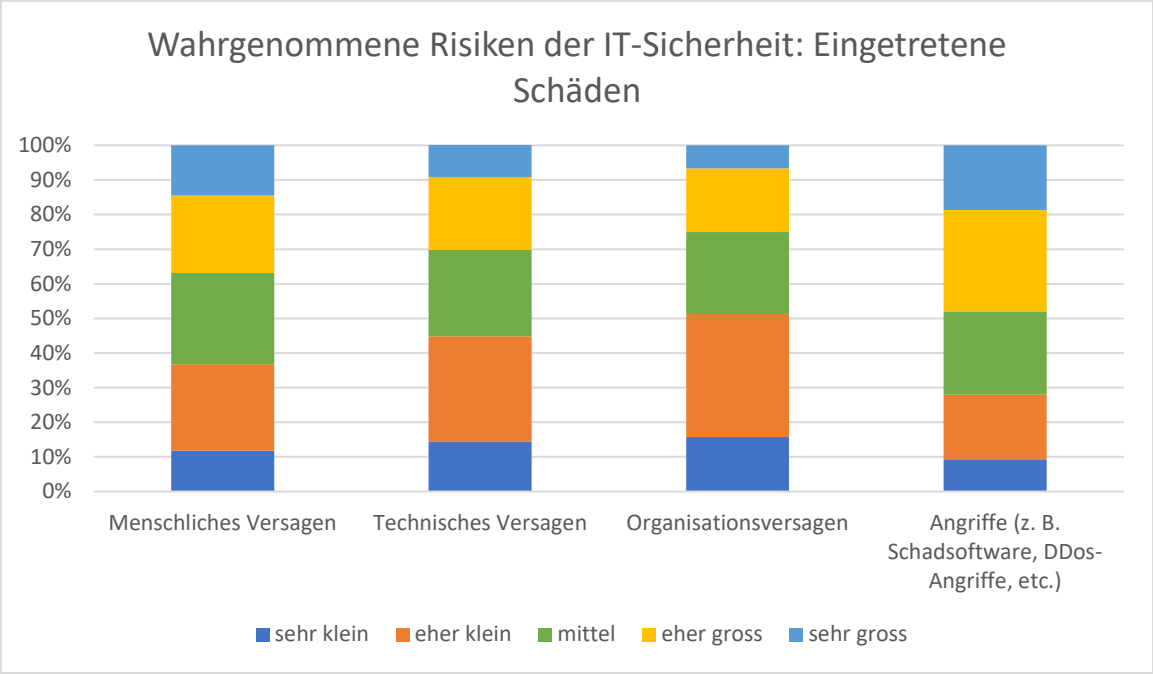

Abbildung 60 – Bewertung des möglichen bzw. tatsächlich eingetretenen Schadens durch die jeweiligen Bedrohungen aus Sicht der KMU.

In der Bewertung des möglichen bzw. tatsächlich eingetretenen Schadens bei den KMU wird der Schaden durch Angriffe und durch menschliches Versagen im Vergleich der Faktoren am signifikantesten eingestuft. Bei der Einzelbetrachtung gaben jeweils 34% der Befragten an, dass sie Angriffe für einen *sehr großen* bzw. *eher großen* Faktor bei möglichen bzw. tatsächlich eingetretenen Schäden halten. Hinsichtlich des Faktors menschliches Versagen gaben 26% der Befragten an, entweder zu einem *sehr großen* oder *eher großen* Maß betroffen zu sein.

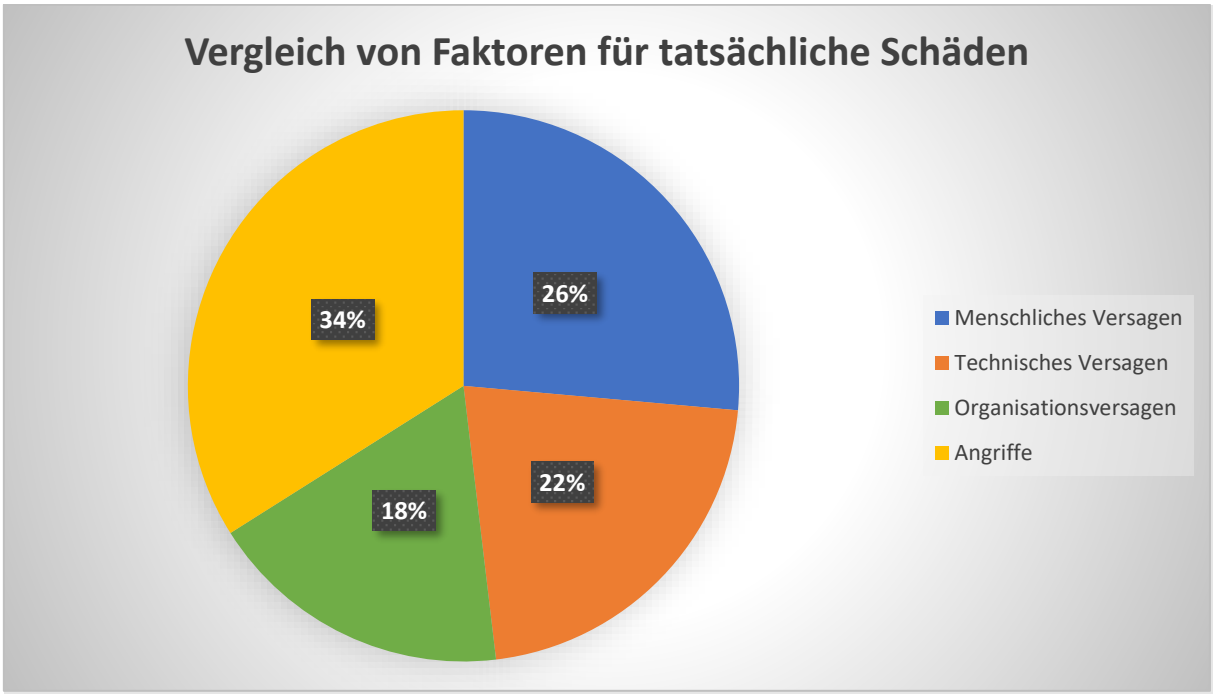

Abbildung 61 – Im Vergleich Bewertung (eher groß bzw. sehr groß) des möglichen bzw. tatsächlich eingetretenen Schadens durch die jeweiligen Bedrohungen aus Sicht der KMU.[156]

Die Antworten geben zu erkennen, dass die Einschätzung mit dem tatsächlichen Wert nicht übereinstimmt. Laut Auskunft der KMU kommen 4% mehr Angriffe, proportional gesehen, für die tatsächlichen Schäden auf. Dafür nimmt der Wert für menschliches Versagen um 8% deutlich ab. Dieses Auswertungsergebnis könnte darauf hindeuten, dass aus Sicht der KMU die momentane Gefahr überwiegend von äußeren Faktoren ausgeht und weniger von mangelnder Sensibilisierung oder Awareness ihrer MitarbeiterInnen. Zumindest zum jetzigen Zeitpunkt scheint menschliches Versagen noch nicht in einem gravierenden Maß die Gefahrenlage der KMU abzubilden. Vielmehr könnten im Zuge des Aufkommens weiterer Entwicklungen, wie die zunehmende Komplexität zum Thema IT-Sicherheit, Fachkräftemangel und Informationslage die KMU dazu veranlasst haben, den Faktor Mensch bei den erwartbaren Risiken höher einzustufen. In der nachfolgenden Grafik sollten KMU angeben, ob sie bereits Opfer eines IT-Angriffs geworden sind. Sie hatten dabei die Möglichkeit, die Frage entweder mit ja, nein oder nicht bekannt zu beantworten. Während 69% der befragten KMU angegeben haben bisher noch kein Opfer eines solchen Angriffs gewesen zu sein, haben weitere 18% einen solchen bereits durchlaufen. Knapp ein Viertel (23%) der TeilnehmerInnen konnte keine Aussagen über einen IT-Angriff auf ihr Unternehmen machen, da ihnen hierzu entweder keine Informationen vorlagen oder nichts bekannt war. Es ist möglicherweise davon auszugehen, dass der Prozentsatz derjenigen Unternehmen, die tatsächlich Opfer eines erfolgten IT-Angriffs gewesen sind, sich auf einem höheren Niveau befindet. Dieser Umstand wäre darauf zurückzuführen, dass die IT-Angriffe bislang von den meisten KMU unentdeckt bleiben. Dies könnte insbesondere auf

[156] Frage: Wie hoch schätzen Sie den möglichen bzw. tatsächlichen eingetretenen Schaden in diesem Bereich durch die aufgeführten Sicherheitsrisiken?

die KMU (82%) zutreffen, die bisher noch keine IT-Angriffe vermeldet haben. Es ist auch nicht außer Acht zu lassen, dass knapp ein Viertel (23%) der KMU keine konkreten Angaben zu eventuellen Vorkommnissen in Bezug auf Ihre IT-Sicherheit machen konnten.

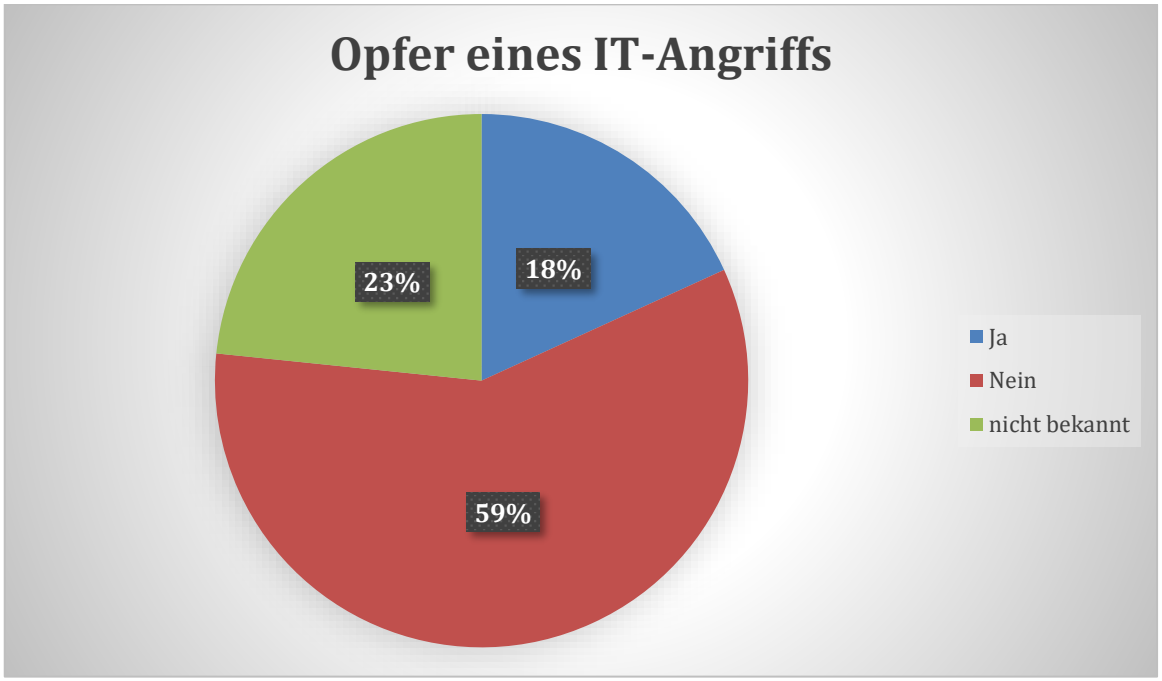

Abbildung 62 – Einschätzung der KMU als mögliches Opfer eines IT-Angriffs.

9.2.6. Besondere Hemmnisse

Bei der Auflistung besonderer Hemmnisse oder Probleme hinsichtlich der IT-Sicherheit der teilnehmenden KMU, wurden vier umfassende Faktoren genannt. Sie können in die Kategorien

1. Kosten
2. Zeitaufwand,
3. Kenntnisse/Qualifikation und
4. Beratung & Vorgehensweise

eingeteilt werden.

Einige der befragten KMU machten deutlich, dass sie die **Kosten** für Einrichtung, Betrieb und Instandhaltung von IT-Sicherheit als hoch erachten. Obgleich der Nutzen dieser Investition nicht in Frage gestellt wird, werden die finanziellen Aufwendungen für Sicherheitseinrichtungen, Virenschutz und Firewall beispielsweise als starke Belastung angesehen. Ferner wurden die laufenden Kosten für Dienstleister und Software wiederholt als zu teuer bezeichnet. Anderen

Aspekten wird zum Teil eine höhere Priorität eingeräumt, weil sie als relevanter für den operativen Betrieb des Unternehmens erachtet werden. Während Investitionen in Produktion oder Vertrieb direkte Mehreinnahmen versprechen, würde das im Falle von IT-Sicherheit nicht zutreffen. Da spezifische IT-Lösungen für Kleinstunternehmen oftmals zu kostspielig sind, muss bei Bedarf auf Standardlösungen zugegriffen werden, die mit einem zusätzlichen administrativen Mehraufwand verbunden sind. Vor diesem Hintergrund wird häufig, wenn nicht zwingend erforderlich, darauf verzichtet. Speziell im Handwerk wird von einer hohen Sensibilität für Preiserhöhungen berichtet, die jegliche Kostenweitergabe an den Kunden schwer vermittelbar macht.

Als weiteres Hemmnis für die Umsetzung einer umfassenden IT-Sicherheitsstrategie wird der benötigte Zeitaufwand, den man zusätzlich zum operativen Geschäft für IT-Sicherheitsmaßnahmen betreiben muss, angesehen. Demnach sehen sich die Unternehmen nicht nur mit immer komplexerer Software und Infrastrukturen konfrontiert, sondern auch mit zeitlichen Restriktionen für die Implementierung grundlegender IT-Schutzverfahren, wie Passwortmanager, Nutzer- und Berechtigungsmanagement. Zusätzlich wird die Aufrechterhaltung der Aktualität der Systeme durch ihre schnelle Weiterentwicklung erschwert. Hierdurch werden kontinuierlich Zeitkapazitäten in Anspruch genommen, die KMU notwendigerweise für die Geschäftsentwicklung aufwenden müssen. Diese „unproduktive“ Tätigkeit wird als Belastung empfunden, die oftmals in den Feierabend verlegt wird, was dazu führt, dass sie nur verspätet oder erst gar nicht durchgeführt wird. Weiterhin wird von einigen TeilnehmerInnen angeführt, dass sie aufgrund der geringen Zahl an MitarbeiterInnen keine/n ausgewiesene/n IT-Zuständige/n vorweisen könnten. Durch diesen Umstand könne keine ausreichende Beschäftigung mit dieser Thematik durch den Rest der Belegschaft sichergestellt werden. Hierzu wurde von einem/r TeilnehmerIn folgende Aussage rezitiert: "IT-Sicherheit ist nicht Alles - aber ohne IT-Sicherheit ist alles nichts“, um es gleich im nächsten Satz zu relativieren: "Das gilt aber auch für vieles andere gleichermaßen". Das Bewusstsein, dass IT-Sicherheit ein relevanter Faktor bei der Unternehmensentwicklung ist, scheint bei vielen Verantwortlichen vorhanden zu sein. Allerdings generieren vor allem präventive IT-Sicherheitsmaßnahmen Kosten und haben bei ausbleibenden Vorfällen keinen eindeutig messbaren Mehrwert (ROSI). Zudem sind Verantwortliche in Kleinstbetrieben mit vielen gesetzlichen Bestimmungen, wie der DSGVO, Arbeitssicherheit, Lohnbuchhaltung und weiteren Anforderungen beschäftigt und vernachlässigen aus diesen Gründen „freiwillige Zusatzaufgaben“, die für viele einen Mehraufwand darstellen, aber nicht als Mehrwert angesehen werden. Wenn Handlungen und Maßnahmen umgesetzt werden sollen, besteht oftmals Unsicherheit über die richtige Vorgehensweise. Die Lage und Bedrohungen sind für KMU eher unübersichtlich, neutrale Beratung ist schwer zu ermitteln und die Bedrohungsquellen sind zu abstrakt.

An dritter Stelle wurden die bekannten Problemfelder, fehlende Kenntnisse bzw. mangelnde Qualifikation im Hinblick auf IT-Sicherheit, detaillierter von den Befragten dargestellt. Wiederholt beschrieben die KMU, dass die Kenntnisse der MitarbeiterInnen zu gering oder rudimentär seien, als dass ein nachhaltiges Verständnis zu dieser Thematik aufgebaut werden könnte. Dies gilt insbesondere auf ein sich dynamisch entwickelndes digitales Umfeld. Einmalige Schulungen sind schnell überholt und das Wissen veraltet. Zudem gaben Handwerksbetriebe beispielhaft an, dass das

Thema „IT-Sicherheit zu umfangreich“ für die Größe der Betriebe seien und dass es deshalb im „Alltagsgeschäft meist untergehe“.

Letztlich wurden von Seiten der Unternehmen die Faktoren **Beratung & Vorgehensweise** mit dem Aufkommen von Hemmnissen, denen sie bei der Umsetzung von IT-Sicherheit begegnen, in Verbindung gebracht. Demzufolge gilt gute Beratung als seltenes Gut und die Neutralität dieser Dienstleistung wird von einigen wenigen dabei in Frage gestellt. Entscheidender sei jedoch der Umstand, dass es keine konkreten Informationen zu vorhandenen Angriffsmustern oder zu Sofort- und Folgemaßnahmen geben würde. Insgesamt wurde bei dieser Frage festgehalten, dass die IT-Sicherheitsinformationen zu allgemein gehalten werden. Daraus würden sich nach Angaben der KMU Unsicherheiten über die Wahl der richtigen Vorgehensweisen für sie ergeben. Konkret wurde folgende Gegenfrage in Bezug zu den Hemmnissen zur IT-Sicherheit gestellt: Welche Prioritäten sollen gesetzt werden?

9.2.7. Öffentliche Förderung

Danach gefragt, welche Erfahrungswerte die KMU mit staatlichen bzw. öffentlichen Fördermaßnahmen gesammelt haben, offenbarten die gewonnen Einschätzungen ein klares Erreichbarkeits- und Bekanntheitsdefizit. Demzufolge erklärten über zwei Drittel (69%) der Befragten, dass sie noch keine Erfahrungen mit staatlichen Unterstützungsprogrammen gemacht haben. Demgegenüber standen 31% der Befragten, die Erfahrungswerte gesammelt haben, aber zu unterschiedlichen Einschätzungen gekommen sind. Hiervon gaben 10% an, überwiegend gute Erfahrungen mit öffentlichen Fördermaßnahmen gemacht zu haben. Die Mehrzahl der KMU mit Erfahrungswerten (15%) schätzte die Fördermaßnahmen nur mit der Aussage *teils/teils* ein. 6% der KMU gaben sogar an, überwiegend schlechte Erfahrungen mit öffentlichen Programmen gemacht zu haben. Die gemachten Angaben geben nicht nur darüber Aufschluss, ob die genutzten Fördermaßnahmen überwiegend als hilfreich wahrgenommen werden, sondern ob diese auch eine breite Akzeptanz unter den KMU finden.

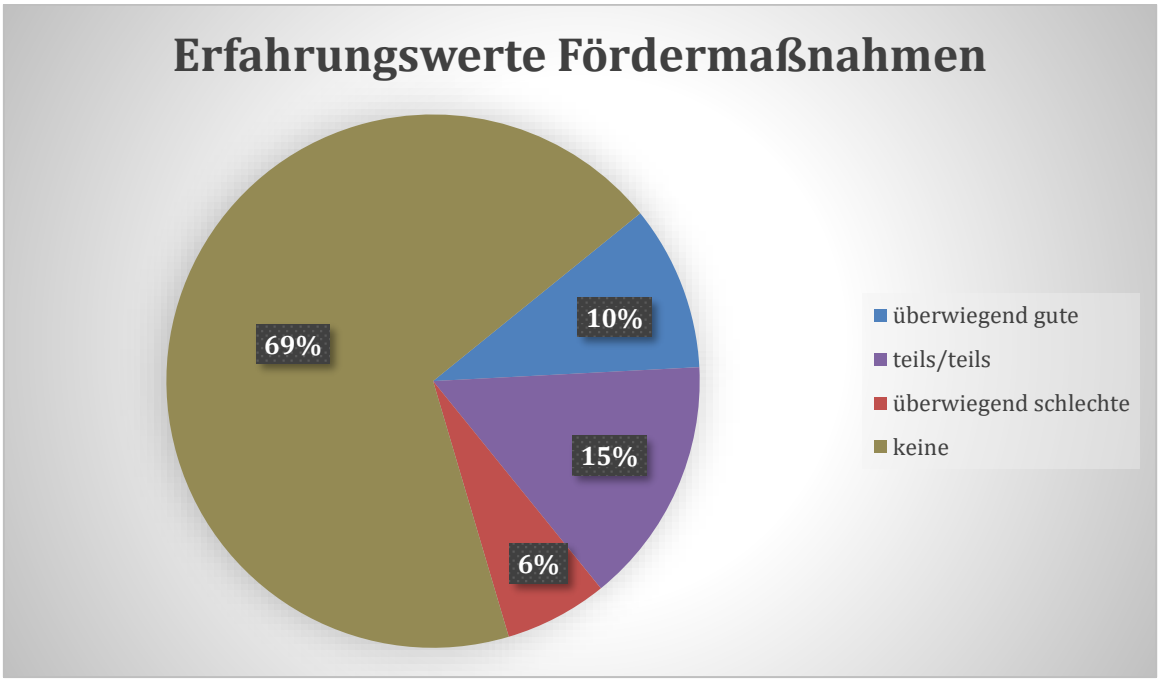

Abbildung 63 – Erfahrungswerte der KMU zu staatlichen bzw. öffentlichen Fördermaßnahmen.

Die Vielzahl existierender Programme im deutschen IT-Bereich reflektiert sich ebenfalls in den Angaben, die die KMU zu der nächsten Frage gemacht haben. Als die Umfragebeteiligten zu ihnen bekannten, staatlichen bzw. öffentlichen Förderprogrammen befragt wurden, ergab sich ein stark heterogenes Bild. Formate wie go-digital (9%) und Digital Bonus Bayern (5%) wurden dabei noch am häufigsten genannt. Gefolgt wurde diese Aufzählung von bekannten öffentlichen Förderungen, z.B. dem IT-Forschungsprogramm des BMBF (3%) oder den aktuellen Förderungen zu Digitalisierungsprämien (3%). Bis auf die Förderprogramme des BMWi (2%) und weiteren Unterstützungsmaßnahmen wie beispielsweise „Digital Jetzt" (2%), können alle weiteren Angaben der KMU unter der Kategorie „ferner liefen" bzw. verschiedene zusammengefasst werden. Knapp der Hälfte der Befragten waren jedoch keine staatlichen Fördermaßnahmen bekannt. Die Auswertungsergebnisse zu den Fördermaßnahmen verfestigen die Annahme, dass das Erscheinungsbild, der Bekanntheitsgrad und die Akzeptanz noch ausbaufähig unter der Zielgruppe der KMU sind.

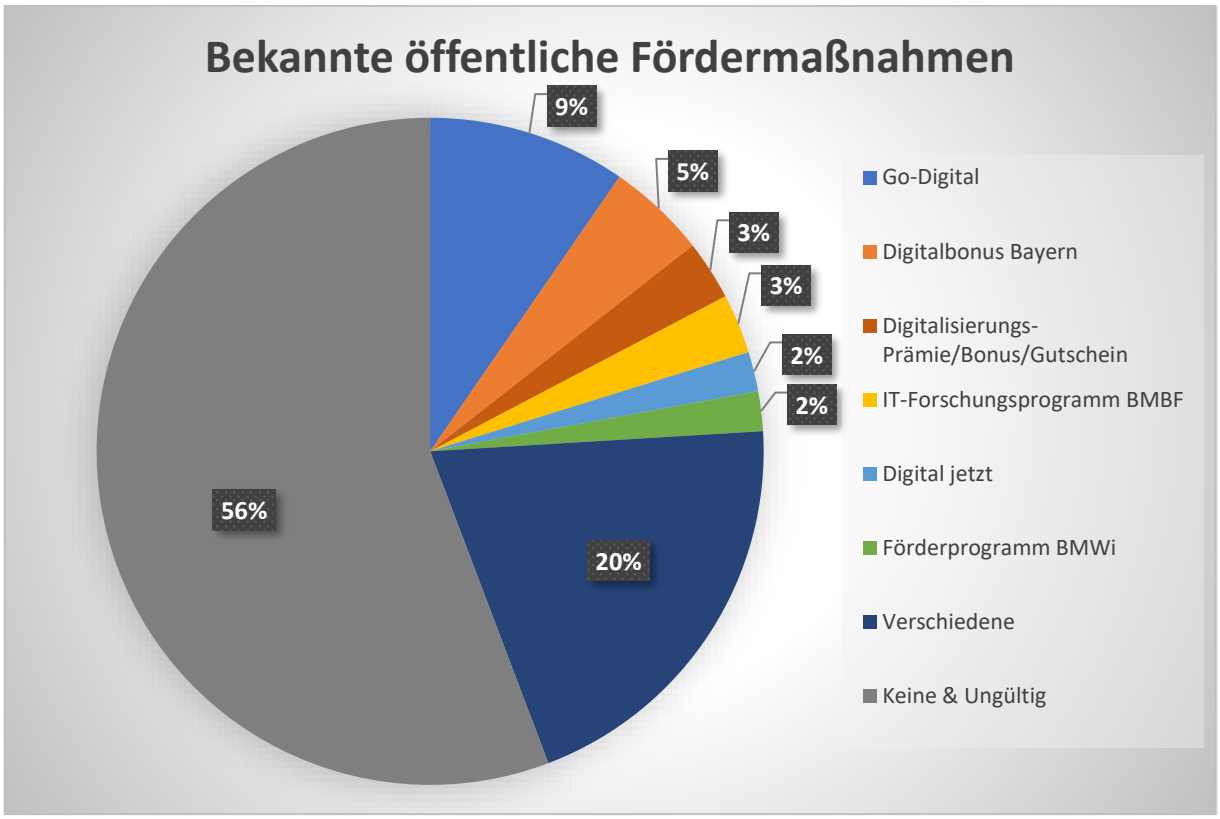

Abbildung 64 – Fördermaßnahmen von Bund und Ländern im IT-Bereich die den KMU bekannt sind.

Zu der Ausgestaltung von Fördermaßnahmen im IT-Bereich lassen sich aus den gemachten Aussagen der KMU vier verschiedene Kategorien unterteilen, die im Nachfolgenden näher betrachtet werden. Diese übergreifenden Kategorien umfassen die Punkte

1. Finanzielle Anreize
2. erleichterter Zugang zu Beratung & Fachexpertise
3. Förderung bei Schulung & Weiterbildung und
4. Etablierung von IT-Schutz- bzw. Sicherheitsstandards.

Zu einem überwiegend hohen Maß und wenig überraschend wären aus Sicht der befragten Unternehmen Fördermaßnahmen in Form von **finanziellen Zuwendungen** wünschenswert. Bei der Ausgestaltung dieser Unterstützung ergibt sich jedoch ein breitgefasstes Bild, das von direkten Subventionen für Beratungsdienstleistungen, über Steuererleichterungen bis hin zu Zuschüssen bei der Inanspruchnahme von externen Dienstleistern reicht. Einzelne Aspekte, wie die Forderung nach einer strukturierten Darstellung dieser finanziellen Fördermaßnahmen, sowie der oftmals geäußerte Wunsch zur Anpassung der Förderkriterien nach Branchen, können hervorgehoben werden.

Unter den gemachten Angaben zur **Beratung & Fachexpertise**, wird insbesondere der Wunsch nach Unabhängigkeit bei Beratungsleistungen zum Ausdruck gebracht. Weitere Vorstellungen sehen von der öffentlichen Hand bereitgestellte Systemüberprüfungen beispielsweise durch unabhängige ExpertenInnen vor. Dabei wird auch ein Vergleich zu einer klassischen Einbruchsschutzberatung gezogen. Des Weiteren wird die Möglichkeit einer Sammelberatung bzw. Gruppenzertifizierung aufgeführt, bei der mehrere KMU parallel und gemeinsam diese Programme durchlaufen könnten. Dies hätte zur Folge, dass der Kostenaufwand für die Vorbereitung solcher Maßnahmen und die anschließende Zertifizierung minimiert wird.

Im Bereich **Schulung & Weiterbildung** wird wiederholt geäußert, eine Förderung zur Erreichung einer größeren Sensibilisierung der MitarbeiterInnen zu erhalten. Dies soll unter anderem dadurch gewährleistet werden, dass IT-Sicherheit auch an Bildungseinrichtungen geschult wird. In einem konkreten Fall wurde auf die Meisterschulen im Handwerk verwiesen. Die Vermittlung von Best Practice-Szenarien als gezielte Fördermaßnahme für Unternehmen, wird als weiterer wichtiger Eckpunkt genannt.

Einige Unternehmen dieser Umfrage zielen auf eine Förderung ab, die die Etablierung von branchenspezifischen **IT-Schutz- und Sicherheitsstandards** für KMU vorsieht. Zumindest sollte eine Übersicht der möglichen Schutzmaßnahmen nach Branchen als Maßnahme für mehr IT-Sicherheit sichergestellt werden. In direktem Zusammenhang dazu steht die Forderung, eine Liste von beispielsweise BSI zertifizierten Anbietern für KMU zur Auswahl zu haben. Gleichzeitig sollten bereitgestellte Leitfäden und Notfallhilfen den KMU im Falle von Angriffen eine bessere Orientierung bieten. Im Sinne dieser Forderung wird eine verbesserte Berichterstattung der IT-Sicherheitslage angeregt. Diese soll den KMU ermöglichen, individuelle Bedrohungsinformationen zu erhalten und ihre IT-Sicherheitsaufstellung danach auszurichten.

9.2.8. Zusammenarbeit mit IT-Dienstleistern

Aus nachfolgender Grafik geht hervor, inwiefern eine Kooperation zwischen externen IT-Dienstleistern und KMU stattfindet. In diesem Zusammenhang sollten die befragten KMU angeben, in welcher Form und bis zu welchem Grad sie mit den externen IT-Dienstleistern zusammenarbeiten, indem sie eine von drei Antwortmöglichkeiten auswählen. Hierzu gaben 50% der Antwortenden an, auswärtige Hilfe zu beanspruchen, wenn sie als notwendig erachtet wird. Die nächstgrößere Gruppe gab im Gegensatz dazu an, keine Zusammenarbeit mit externen Dienstleistern im IT-Bereich zu praktizieren, sondern ausschließlich auf Inhouse-Lösungen zu setzen. Mit 22% gab die dritte Gruppe der KMU an, entweder weitgehend oder vollständig ihre IT-Sicherheit outzusourcen. Die Beweggründe zur Auswahl einer der genannten Gründe, können dabei nicht abgeleitet werden. Es kann nur gemutmaßt werden, dass finanzielle Erwägungen und die allgemeine IT-Affinität des Unternehmens eine entscheidende Rolle gespielt haben.

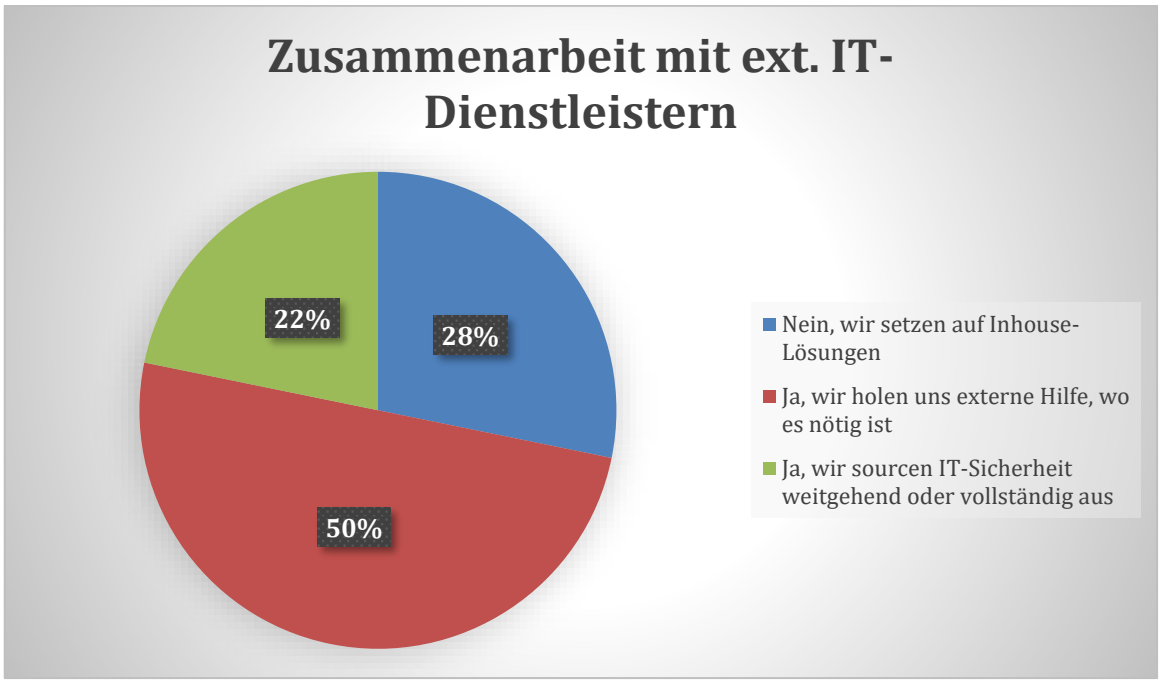

Abbildung 65 – Zusammenarbeit der KMU mit externen Dienstleistern.

Zu der Frage, welche weiteren Aspekte aus Sicht der KMU für den IT-Sicherheitsbereich noch wichtig wären, wurden insgesamt zehn übergreifende Punkte von den TeilnehmerInnen genannt. Darunter fielen einige Aspekte, die in den Fragen zuvor bereits behandelt wurden, aber an der Stelle weiter in Detail und im Einzelnen ausgeführt werden.

Einige der Befragten sehen eine **kostenfreie Unterstützung**, sei es zur Klärung von grundlegenden Fragen im IT-Bereich oder in Form von finanziellen Förderungen eines IT-Sicherheitsberaters, als eine wünschenswerte Maßnahme an. Ferner werden von einigen Programme gefordert, die sich mehr an den sich verändernden Rahmenbedingungen orientieren. Insbesondere werden **gezielte Finanzierungsmodelle** gewünscht, die auf die Unternehmensgründungsphase abzielen, da von Seiten der Kunden oftmals IT-Vorgaben eingehalten werden müssen. Diese Auflagen würden gerade in der Anfangsphase viel Kapital der Kleinstunternehmen binden, das oftmals anderweitig eingesetzt werden muss.

In Bezug auf die sich verändernden gesetzlichen Rahmenbedingungen müsste außerdem eine regelmäßigere **Validierung** von Seiten einer zentralen Koordinierungsstelle, die sich ausschließlich um Belange der KMU kümmern, durchgeführt werden. So könnte sichergestellt werden, dass die **gesetzlichen Anforderungen** für Klein- und Kleinstbetriebe bekannt und umsetzbar bleiben.

Es wurde mehrmals der Wunsch nach mehr **Verständlichkeit** und **überschaubareren Umsetzungsmöglichkeiten** von Programmen ausgedrückt. Dieser Forderung wurde gerade dann Nachdruck verliehen, wenn kein/e IT-MitarbeiterIn im Unternehmen beschäftigt wird. In diesem Zusammenhang wurden **Best Practice Szenarien** gewünscht, die den KMU leicht umsetzbare Maßnahmen zur Verbesserung ihrer IT-Sicherheit bieten. Bereitgestellte Handlungsempfehlungen würden oftmals nicht zweckdienlich sein, da sie sich nicht als konkrete bzw. **praktikable Lösung** erweisen. Einige

TeilnehmerInnen verwiesen auf die Notwendigkeit, **Entscheidungshilfen** bei der Verwendung von automatisierten Sicherheitstools und interaktiver Leitfäden (z.B. Einführung eines ISMS) durch öffentliche Institutionen bereitzustellen. Damit einhergehend werden von einzelnen befragten KMU **regelmäßige Informationen** zu kritischen Sicherheitsproblemen, Bedrohungslagebilder und individualisierte Bedrohungsinformationen, speziell für KMU, erwartet.

Zu den weiteren genannten Aspekten gehört die Schaffung von Anreizen zur Wahrnehmung **kostengünstiger Aus- und Weiterbildungsmöglichkeiten** im Bereich IT-Sicherheit für KMU. Diese Anreize würden ihrer Meinung nach erlauben, vermehrt auf QuereinsteigerInnen zu setzen und damit IT-Personal zu geringeren Kosten zu akquirieren.

9.3. Wesentliche Erkenntnisse aus der qualitativen und quantitativen Befragung der KMU

9.3.1. Verschiedene KMU Kategorien

Sowohl die qualitative wie auch die quantitative Befragung zeigen deutlich, dass man KMU in Bezug auf ihre IT-Sicherheitsaufstellung nicht als eine homogene Gruppe betrachten kann. Dazu ist die Gruppe bezüglich ihrer Wirtschaftskennzahlen, Produkte, Services und Marktausrichtung zu divers aufgestellt. Man kann demnach nicht von „den KMU" im Kontext der IT-Sicherheit sprechen. Es muss stattdessen eine klare Differenzierung hinsichtlich ihres Auseinandersetzungsgrads mit IT-Sicherheit, die sich aus den Anforderungen der Digitalisierung der Geschäftsmodelle ergibt, gemacht werden. Dabei konnte aus der Auswertung der Interviews eine Kategorisierung in vier verschiedene KMU-Typen vorgenommen werden. Die befragten Unternehmen werden hiernach in jene beiden Kategorien eingeteilt, die sich entweder fortlaufend und regelmäßig mit der IT-Sicherheit beschäftigen und sich diesbezüglich auch klar positionieren. Während die anderen zwei KMU-Kategorien sich in angepasster oder oftmals in unzureichend bzw. mangelhafter Weise mit IT-Sicherheit auseinandersetzen.

Wenig überraschend fallen zumeist Kleinstunternehmen in die Kategorie der gefährdetsten KMU, da sie mit strukturellen Nachteilen zu kämpfen haben. Die offensichtlichsten Nachteile umfassen oft eine ablehnende Einstellung zum Thema IT-Sicherheit oder ihre mangelnde Durchsetzung durch die Geschäftsführung. Zudem schließen diese Nachteile, die oftmals ausgeprägte Abhängigkeit von Ein-Personen-IT-Dienstleistern (SystemadministratorInnen), wie in den Befragungen geschildert, mit ein. Die ablehnende Haltung, wie dargelegt, geht häufig mit einer passiven statt proaktiver Zusammenarbeit der KMU mit den Dienstleistern einher. Ebenso hat sich gezeigt, dass es gerade für kleinere KMU eine Herausforderung ist, Anbieter für angefragte oder ausgeschriebene Leistungen zu finden. Hierzu merkten die interviewten KMU an, dass sich eine Steigerung der Attraktivität als Arbeitgeber potenzieller IT-MitarbeiterInnen durchaus erzielen lässt. Ein individuell zusammengestelltes Kundenportfolio könne demzufolge und im Hinblick auf den Fachkräftemangel in der IT-Branche einen starken Anreiz schaffen, für das Unternehmen zu arbeiten. Nichtsdestotrotz konnten noch weitere Faktoren identifiziert werden, die unabhängig der Größe des KMU, für eine zögerliche Umsetzung von IT-Sicherheit in den Unternehmen sorgen können, auf die im Folgenden eingegangen wird.

9.3.2. Risikofaktor Mensch

Der Faktor Mensch stellt sich in den Auswertungen als eines der größten Risiko- bzw. Sicherheitsfaktoren für die IT-Sicherheit von KMU heraus. Dies bestätigt sowohl die qualitative als auch die quantitative Befragung der KMU. Wenngleich das Ausmaß (26% siehe Abbildung 58) nach der quantitativen Auswertung niedriger angesetzt werden muss als bei der Befragung von IT-Dienstleistern. Externen Angriffen (siehe 34% Abbildung 60) auf die IT der KMU wurde beim Eintreten tatsächlicher Schäden ein noch höherer Stellenwert beigemessen. Dieser Umstand könnte jedoch in erster

Linie der eigenen subjektiven Wahrnehmung und Überschätzung durch Erwünschtheit geschuldet sein. Somit dürfte es sich aller Voraussicht nach auch mit der Einschätzung zur eigenen Opferwahrnehmung verhalten. Gleichzeitig wird vom Faktor Mensch perspektivisch (34% siehe Abbildung 58) eine wachsende Gefahr für eine erfolgreiche Fortsetzung der Geschäftstätigkeit der Unternehmen erwartet.

So findet oftmals laut der Interviews keine Trennung der verwendeten Daten aus Arbeits- und Privatleben statt. Es wird als weiterer Beleg für das Zustandekommen illegaler Zugriffe darüber berichtet, dass der Gebrauch unsicherer Anwendungen zur Aufrechterhaltung der Geschäftstätigkeit in Kauf genommen wird. Besonders kritisch ist in diesem Zusammenhang die praktizierte „Augen zu und durch"-Mentalität für die IT-Sicherheitsaufstellung der KMU zu erachten. Hierdurch wird nicht nur der eigene, sondern der Schutz und die Daten sämtlicher Stakeholder in Gefahr gebracht. Menschliches Verhalten beeinflusst nicht nur geschäftsrelevante Aspekte, wie die Anpassung und Optimierung von Organisationsprozessen. Es offenbart zugleich ein weiteres Kernproblem der KMU: Die finanzielle Positionierung zu IT-Sicherheit. Zunächst wird jedoch auf die Vorgehensweisen und Organisationsprozesse eingegangen.

9.3.3. Geschäftsprozesse, Problemumgang und Information

Ein grundlegendes Problem, welches sich aus den Interviewaussagen des qualitativen Teils der Auswertung ergibt, stellt die Vermittlung und das Verständnis für die integrale Überführung aller wesentlichen Geschäftsprozesse in eine von Anfang an durchdachte IT-Sicherheitsarchitektur (Stichworte "security by design und security by default"), dar. An der Stelle wird nach Meinung vieler TeilnehmerInnen noch von öffentlicher Seite zu wenig getan, um das Verständnis in sämtlichen Branchen, auch jene des produzierenden Gewerbes, stärker dafür zu sensibilisieren.

In Verbindung zu dieser Aussage kann die Auswertung aus der quantitativen Befragung herangezogen werden. Sie zeigt, dass ein Drittel entweder keine oder nur rudimentäre Regelungen im Falle eines Vorfalls vorlegen kann. Als Gründe für die schwache IT-Sicherheitsaufstellung werden wiederholt von TeilnehmerInnen fehlende Verständlichkeit der erforderlichen Maßnahmen genannt. Hier könnten auch überschaubarere Umsetzungsmöglichkeiten bzw. praktikablere Lösungen eine höhere IT-Sicherheit erzielen.

Die aufzuwendenden Zeiten und Mittel zur Gewährleistung der IT-Schutzfunktionen werden bislang nicht in hinreichender Form bereitgestellt. Der Aufwand hierfür wird häufig als zu hoch bezeichnet. Weitere in Zusammenhang mit dem Umgang von IT-Sicherheit stehende Gesichtspunkte sind die Regelmäßigkeit, mit der sich die IT-Verantwortlichen im Unternehmen beschäftigen sowie die Informationsbeschaffung zu IT-Sicherheit. Sie liefern weitere Erkenntnisse darüber, welche Stellung das Thema IT-Sicherheit im Unternehmen einnimmt. Es hat sich dabei gezeigt, dass sich noch immer ein wesentlicher Teil, knapp 40% (siehe Abbildung 55), nicht laufend oder zumindest in monatlichen Abständen, sondern nur bei Bedarf, informiert hält.

9.3.4. Finanzielle Implikationen

Sowohl die qualitative als auch die quantitative Umfrage haben verdeutlicht, dass finanzielle Erwägungen beim Thema IT-Sicherheit näherer Aufmerksamkeit bedürfen. Hier zeigen die Ergebnisse, dass der Anteil aus dem für IT-Sicherheit zur Verfügung stehenden IT-Budget bei einem Großteil der KMU noch deutlich zu gering ist. Während ein sehr geringer Teil der KMU ihren hohen Anteil des IT-Budgets für IT-Sicherheit aufwendet, verharrt der Rest (88% siehe Abbildung 51) auf einem unteren Niveau zwischen 0 bis 30%. Tendenziell liegt die Bereitschaft der KMU vor, einen höheren prozentualen Wert von ihrem IT-Budget für externe IT-Dienstleister aufzubringen. Insbesondere wenn man sich den Wert derjenigen Unternehmen (22%, siehe Abbildung 52) vor Augen führt, die bereit sind, zwischen 31 und 100% des IT-Budgets dafür zu reservieren. Verstärkt wird der Eindruck der suboptimalen Finanzierung im IT-Sicherheitsbereich durch den Umstand, dass gerade einmal 7% (siehe Abbildung 53) der KMU angegeben haben, dass sie über ein speziell ausgewiesenes Budget für diesen Bereich verfügen.

Die Ergebnisse aus den Interviews zeigen, dass die Aussicht auf Kosteneinsparpotentiale in Bezug auf die IT KMU teilweise dazu bewogen haben, unterschiedliche Dienstleister mit Teilaufgaben zu beauftragen. Dadurch entstehen Kompatibilitätsprobleme, die sich nachteilig auf die IT-Sicherheitsaufstellung auswirken. Dies widerspricht auch einem Grundsatz bei der Inanspruchnahme von IT-Dienstleistungen, möglichst Leistungen aus einer Hand zu beziehen und Schnittstellen zu minimieren. Auf Seiten der KMU würde sich durch die zielgerichtete Ausweitung der IT-Aufwendungen und Bündelung von Dienstleistern eine Risikominimierung ergeben. Hierdurch könnten sie die Risiken, Opfer eines geschäftslähmenden und damit kostspieligen Angriffs zu werden, minimieren. Eine zuverlässige und robuste Informations- und Kommunikationstechnik eines Unternehmens ist jedoch mit einer vernünftigen Investitionstätigkeit im IT-Bereich, einer ganzheitlichen Betrachtung des eigenen Informationsverbunds und angemessenen Schutzmaßnahmen verknüpft.

9.3.5. Öffentliche Förderung und gesetzliche Rahmenbedingungen

Die Erwartungshaltung an die öffentliche Hand bei der Erbringung von Förderleistungen, insbesondere der kleineren KMU, ist groß. Dies zeigt sich anhand der durchwachsenen Erfahrungswerte der Befragten mit der Vielzahl an Förderprogrammen. Gerade einmal 10% (siehe Abbildung 63) der TeilnehmerInnen schätzte diese überwiegend positiv ein. Weitere 21% schätzten die Auslegung der Förderprogramme als teils/teils oder gar als überwiegend schlecht ein. Ferner ließ die Abfrage der Bekanntheitsgrade Zweifel an der Visibilität und Akzeptanz der Fördermaßnahmen aufkommen. Bis auf die Programme „go-digital“ (9%, siehe Abbildung 64) und „Digitalbonus Bayern“ (5%) konnten gerade einmal 30% der KMU weitere Fördermaßnahmen mit der konkreten Programmbezeichnung angeben.

Es hat sich bei den nähergehenden Fragen zur potenziellen Ausgestaltung der Unterstützungs- und Anreizmaßnahmen außerdem herausgestellt, dass es zum Teil deutliche Kritikpunkte an diesen gibt. Die wichtigsten gemachten Verbes-

serungsvorschläge zielten auf die Feststellung ab, dass die bestehenden Förderprogramme oftmals nicht einer breiteren KMU-Gruppe zugänglich seien. Durch die Komplexität der Materie entstand der Eindruck, dass nur spezifische Bereiche als förderwürdig erachtet werden. Diese Wahrnehmung ging mit der Feststellung einher, dass die Auflagen zur Teilnahme an Förderprojekten als zu restriktiv und zu bürokratisch bezeichnet wurden. Insgesamt wurde der dringliche Wunsch nach einer strukturierteren Darstellung der zur Verfügung stehenden Maßnahmen und ihrer Kriterien geäußert. Somit könnten gewünschte Förderungen aus dem Bereich Aus- und Weiterbildung, Beratung, Fachexpertise und Umsetzung besser abgerufen werden.

In Bezug auf die gesetzlichen Rahmenbedingungen ergab sich aus den Rückmeldungen, dass den KMU an einer zentralen Koordinierungs- und Kontakt- bzw. nahbaren Beratungsstelle gelegen wäre. Hiernach könnte eine solche Anlaufstelle branchenspezifische Sicherheitsstandards sowie sich ändernde regulatorische Umstände einbeziehen und befördern. Die genannten Punkte lassen entscheidende Lenkungsmöglichkeit des Bundes und der Länder beim Erfolg der KMU zur Umsetzung von IT-Sicherheit in ihren Unternehmen erkennen.

10. Handlungsempfehlungen

Die folgenden Handlungsempfehlungen greifen die Analysen der vorherigen Kapitel mit der engen Ausrichtung auf die wirtschaftspolitischen Ziele und die Forschungsfrage dieser Studie auf. Sowohl die Angebotsseite der IT-Dienstleister als auch die Nachfrageseite der KMU werden in den Handlungsempfehlungen berücksichtigt.

Die Handlungsempfehlungen sind in 5 Handlungsfelder geclustert und um ein querschnittliches, koordinierendes Handlungsfeld ergänzt.

Abbildung 66 – Zusammenfassende Darstellung der Handlungsfelder der Studie

Somit wurden die Handlungsempfehlungen auf die folgenden Schwerpunkte ausgerichtet:

- Schaffung einer stetig aktualisierten **Übersicht** über die Bedrohungslage im Cyberraum für KMU sowie über Risiken und Schutzmöglichkeiten (Handlungsfeld 1)
- Verbesserung des **Informationsaustauschs und Wissenstransfers** der beteiligten Akteure für eine effektivere und effiziente Entscheidungsfindung (Handlungsfeld 2)
- Erhöhung des **IT-Sicherheit-Know-hows bei Führungs- und Fachkräften** in den KMU (Handlungsfeld 3)
- Schaffung von **Anreizen für mehr IT-Sicherheit** durch eine effektive Förderung und eine Senkung von Suchkosten für KMU bei der Wahl des IT-Dienstleisters (Handlungsfeld 4)
- Verstärkte Etablierung von **Qualitätskriterien und IT-Sicherheitsstandards** (Handlungsfeld 5)

- Das querschnittliche Handlungsfeld soll eine **begleitende Koordinations- und Kommunikationsstrategie** unterstützen, um die Studienergebnisse kontinuierlich umsetzen zu können.

Eine Strategie zur Verbesserung der Rolle der IT-Dienstleister für mehr Sicherheit bei KMU kann nur funktionieren, wenn die genannten Empfehlungen, Kompetenzen und Prozesse unter Berücksichtigung der Akteure langfristig ausgerichtet und weiterentwickelt werden. Keiner der beteiligten Akteure (IT-Dienstleister, KMU, öffentliche Hand) kann diese Handlungsfelder allein umsetzen.

Auf Ebene der einzelnen Handlungsempfehlungen wurde eine Vielzahl an Maßnahmen entwickelt, die dazu dienen sollen, die genannten Ziele zu erreichen. Die Maßnahmen sollten in einem Beteiligungsprozess mit möglichen Trägern der Maßnahmen diskutiert und von diesen im Sinne einer Aufgabenteilung umgesetzt werden.

Damit setzen die Handlungsempfehlungen einen Rahmen für eine gebündelte und abgestimmte Vorgehensweise.

Die Handlungsempfehlungen und die strategische Ausrichtung sollten in einem Beteiligungsprozess regelmäßig überprüft und bei Bedarf angepasst werden. Hierbei kann das querschnittliche Handlungsfeld unterstützen.

10.1. Handlungsfeld 1: Lagebild und Risikomanagement

Empfehlung 1.1	***Lagebild und verlässliche Informationen über Art und Umfang der aktuellen, digitalen Bedrohungen für KMU***
Ziel	- Holistisches Bild der Bedrohungslandschaft für KMU (Informationen müssen für KMU aufbereitet werden, da nicht zielgerichtete Informationen häufig zu einer Art "Handlungslähmung" durch Informationsüberflutung führen). - Realistischere Einschätzung der Bedrohungslage, um darauf basierend geeignete Gegenmaßnahmen zum Schutz treffen zu können. - Quantitative und qualitative Entscheidungsunterstützung für IT-Dienstleister und damit mehr Sicherheit für KMU.
Maßnahmen	- Zeitreihendaten müssen geführt werden, um Korrelationen zwischen der Angriffsmethode und dem Angriffsziel ableiten zu können. - Austausch zwischen IT-Dienstleistern, IT-Sicherheitsunternehmen, KMU und Fachbehörden, um Bedürfnisse der KMU zu eruieren und digitale Bedrohungsinformationen gezielt aufbereiten zu können. - Trendanalysedaten auf Basis der bereitgestellten Daten von KRITIS Betreiber (IT-Sicherheitsgesetz), IT-Sicherheitsdienstleistern und Fachbehörden (z.B. BSI oder auch Landesbehörden).
Verweise	7.1.1, 7.2.2, 7.2.6, 7.2.8, 9.1.5.3, 9.2.2

Empfehlung 1.2	*Erhöhung der Bedeutung des Risikomanagement und der Bekanntheit von Risikotools*
Ziel	- IT-Sicherheitsmaßnahmen sind immer ein Ergebnis von Bedrohungsanalysen und Risikobewertungen der eigenen IT-Infrastruktur und des IT-Verbunds. Risikobetrachtungen ermöglichen auch einen priorisierten Ansatz bei der Umsetzung von IT-Sicherheitsmaßnahmen im eigenen Unternehmen. - Anwendbare und auf KMU-Belange ausgerichtete Risikotools, -modelle und -profile mit praktikablen Handlungsanweisungen und Schutzmechanismen für KMU-spezifische IT-Verbünde können somit eine große Hilfe bei der Planung von IT-Sicherheitsmaßnahmen für KMU darstellen. - Die KMU müssen verstärkt befähigt werden, gemeinsam mit ihren IT-Dienstleistern, individuelle Risikoprofile für das eigene Unternehmen unter Berücksichtigung der eigenen Bedrohungslage zu nutzen, bei Bedarf zu erstellen und umzusetzen.
Maßnahmen	- Bessere und aktuelle Informationen zu(m) Risikomanagement, -tools, - modellen und zu Risikoprofilen (z.B. Branchenprofile, nach Unternehmensgrößen, nach Betrachtung des Informationsverbunds). - Die Selbsteinschätzung bezüglich Bedrohungen und IT-Sicherheitsrisiken in den KMU muss gestärkt werden. - Stärkung und Bereitstellung von branchenspezifischen und KMU-ausgerichteten Muster-Risikoprofilen unter Einbindung der IT-Dienstleister, deren Netzwerke, von Verbänden und Transferstellen
Verweise	7.1.1, 7.2.2, 7.2.3, 9.1.5.2, 9.2.1, 9.2.3, 9.2.5, 9.3.2, 9.3.3

Empfehlung 1.3	*Stärkung der Rolle von Cyberversicherungen für KMU als Baustein des Risikomanagements*
Ziel	- Der Abschluss von Cyberversicherungen führt dazu, dass sich die Unternehmen vor dem Abschluss der Versicherung mit den bestehenden IT-Sicherheitsrisiken organisatorisch und technisch befassen müssen. IT-Dienstleister sollten verstärkt die Versicherungen als einen Baustein des IT-Risikomanagements berücksichtigen. - Im Schadensfall stellt die Versicherung dem KMU und seinem IT-Dienstleister häufig notwendige Notfall und IT-SicherheitsexpertInnen zur Seite (Assist-Leistungen). - Haftungsrisiken von IT-Dienstleistern können begrenzt werden. - Präventive Maßnahmen werden durch die Prüfungen der Versicherungen vor Abschluss analysiert. - Während der Versicherungsdauer können laufende Prüfungen erfolgen, um den jeweils aktuellen Stand der IT-Sicherheit nachzuweisen (entsprechend der jeweiligen Bedingungen von IT-Sicherheitspolicen).
Maßnahmen	- Verstärktes Matching von Versicherungsgesellschaften bzw. MaklerIn mit IT-Dienstleistern, um Versicherungen als Baustein des Risikomanagements zu etablieren.

	- Wahrnehmung der verstärkten Schulungsangebote von Versicherungen für Geschäftsführung von KMU und für IT-Sicherheitsverantwortliche in KMU - Schulungsangebote können mit Demonstrationen durch externe Dienstleister, die im Notfallmanagement durch die Versicherungen eingesetzt werden, angereichert werden. - Bundesweite Vernetzung und Ausbau von Awareness-Angeboten für KMU Erfahrungsaustauch mit betroffenen Unternehmen und ggfs. Moderation der Versicherungen
Verweise	7.1.1, 7.2.6, 9.2.6

10.2. Handlungsfeld 2: Informationsaustausch und Wissenstransfer

Empfehlung 2.1	***Aufbau von bundesweiten und möglichst regionaler Ansprechstellen für eine Erst-hilfe bei IT-Vorfällen und -Notfällen für KMU***
Ziel	- Ergänzend zu bestehenden oder im Aufbau befindlichen Zentren und Transferstellen zur Wissensvermittlung, mit Informationsangeboten und konzeptionellen Lösungen, muss der Aufbau von Ansprechstellen mit einem Unterstützungsangebot im Ereignisfall (sog. Notfall-Hotlines) in Deutschland erfolgen. - Neben dem Aufbau solcher Hotlines müssen Standards zur Servicequalität etabliert werden. - Privat und Staat müssen an dieser Stelle in eine Symbiose treten. Während die Strafverfolgung, z.B. in Form der Zentralen Ansprechstellen Cybercrime (ZAC) der Polizeien, eine staatliche Aufgabe ist, gehört die Prävention und Schadensbegrenzung/Eindämmung zu den gemeinschaftlichen Aufgaben. Staatliche Stellen wie die Transferstelle IT-Sicherheit im Mittelstand (TISiM) z.B., können eine Hilfestellung bei der Bedarfsermittlung der IT-Sicherheit leisten und bei der Umsetzung unterstützen, allerdings sind konkrete Maßnahmen von der Privatwirtschaft umzusetzen. Gleiches gilt bei der Schadensbegrenzung/Eindämmung von Cybervorfällen. Die Aufklärung durch z.B. zentrale Stellen wie das BSI oder regionale Einrichtungen wie z.B. die Digitalagenturen der Länder, fallen in den staatlichen Aufgabenbereich, die Umsetzung jedoch ist eine private Aufgabe und schließt IT-Dienstleister, die nah an den KMU dran sind, unbedingt mit ein.[157]
Maßnahmen	- Verstärkter Aufbau von einer Notfall-Hotline mit zentraler Erreichbarkeit und Vermittlung von regionalen IT-Sicherheitsdienstleistern - Erweiterung bestehender Serviceangebot bei Transferstellen, Mittelstandszentren, IHKn, Handwerkskammern, Verbände, Gremien und Netzwerken - Erarbeitung von Qualitätsstandards für Notfall-Hotlines (für Services und auch Personal in den Hotlines)
Verweise	7.2.8, 7.3.6, 9.1.5.2, 9.2.8, 9.3.1

[157] Vgl. Bretschneider et al. 2020, S. 105 ff.

Empfehlung 2.2	*Zentrale Anlaufstelle für Förderprogramme für mehr IT-Sicherheit bei KMU*
Ziel	- Suchaufwand für Förderprogramme mit IT-Sicherheitsrelevanten Inhalten reduzieren, um zielgerichtete Programme durch Bedarfsanalyse zu finden. - Transparenz der Förderlandschaft erhöhen - Anlaufstelle sollte sich auch als Service für IT-Dienstleister verstehen.
Maßnahmen	- Bestehende Strukturen durch mehr Kooperation, mehr Ressourcen und einer umfangreichen digitalen und analogen Kampagne (zur Bekanntmachung) stärken. - KMU und Netzwerke der IT-Dienstleister in jährliche Workshops der zentralen Anlaufstelle (z.B. TISiM) integrieren, um Feedbackschleifen zu etablieren und Angebot agil (angepasst) zu gestalten. - Zielgruppengerechte Ansätze und Angebote entwickeln
Verweise	7.2.8, 7.3.6, 9.1.5.2, 9.2.7, 9.3.5

10.3. Handlungsfeld 3: Fachkräfte und Personalressourcen

Empfehlung 3.1	*IT-Sicherheitswissen bei Führungs- und Fachkräften in KMU stärken*
Ziel	- Bei KMU muss die Anzahl der MitarbeiterInnen und Führungskräfte mit IT-Sicherheitskenntnissen erhöht werden. - Selbst wenn für die meisten KMU IT-Sicherheit nicht Teil des Kerngeschäfts ist, können IT-Sicherheitsvorfälle häufig unternehmensgefährdende Auswirkungen haben. Aus diesem Grund muss sowohl die Qualifikation und auch die Sensibilisierung der verantwortlichen MitarbeiterInnen weiter erhöht werden.
Maßnahmen	- Verstärkte Informationen zu Aufgaben von IT-Sicherheitsleitlinien und der Rolle der Geschäftsführung für die IT-Sicherheit im Unternehmen - Verstärkte Schulungsangebote zur Rolle der Geschäftsführung für IT-Sicherheit - Bundesweite Vernetzung und Ausbau von Awareness-Angeboten für KMU - Verpflichtende Beratung in IT-Sicherheitsfragen auf Geschäftsleitungsebene bei Inanspruchnahme von Förderprogrammen zur Digitalisierung
Verweise	7.1.1, 7.2.8, 7.3.1, 9.1.5.2, 9.2.1, 9.2.3, 9.2.4, 9.3.2, 9.3.3

-

Empfehlung 3.2	*Etablierung von Einweisungen und regelmäßige Auffrischungskurse und Serviceangebote für KMU-MitarbeiterInnen zum Thema IT-Sicherheit*
Ziel	- Die KMU-MitarbeiterInnen wissen über die Gefahren durch Cyberangriffe Bescheid und handeln entsprechend der IT-Sicherheitsregeln des Unternehmens. - Durch regelmäßige Auffrischungskurse bleiben die MitarbeiterInnen über die sich dynamisch verändernden Gefahren einschließlich entsprechender Vorsichtsmaßnahmen informiert.

Maßnahmen	- Nutzung digitaler Schulungswerkzeuge (z.B. kurze Videos, Online-Schulungen) bei der Durchführung der Maßnahmen - Schaffung einer Plattform mit Angeboten und transparenten Qualitätskriterien (Markttransparenz) - Bündelung vorhandener Awareness-Plattformen mit der Nachfrageseite der KMU auf dieser Plattform (Suchkosten senken)
Verweise	7.1.1, 7.2.8, 7.3.1, 9.2.5, 9.2.6, 9.3.2

10.4. Handlungsfeld 4: Förderung

Empfehlung 4.1	***Förderung zur Umsetzung von IT-Sicherheitsmaßnahmen und -investitionen***
Ziel	- Der Fokus der bestehenden Förderungen liegt auf Beratungs- und reine Serviceleistungen. Die für die Umsetzung notwendigen Investitionen, z.B. in Hard- und Software, sollten stärker berücksichtigt werden. - Ähnlich wie in anderen Bereichen (z.B. Gebäudesicherheit) sollte die Umsetzung der erforderlichen technischen Maßnahmen stärker beachtet werden. - Umsetzung der IT-Sicherheitsmaßnahmen könnte somit erleichtert und externe Effekte kompensiert werden.
Maßnahmen	- Verstärkte Förderung der Umsetzung geeigneter IT-Sicherheitsmaßnahmen einschließlich der Investitionen für Hard- und Software - Prüfung der Anpassung weiterer Instrumente, z.B. AfA-Tabellen (Verkürzung Abschreibungszeiten) - Gegebenenfalls Förderung von Beratungsleistung nur gewähren, falls eine Umsetzung der Maßnahmen erfolgt.
Verweise	7.1.2, 7.2.8, 7.3.5, 7.3.6, 9.2.3, 9.2.6, 9.2.7, 9.3.5

Empfehlung 4.2	***Stärkung der Kompetenzen der IT-Dienstleister im Bereich Förderprogramme***
Ziel	- Die IT-Dienstleister sind in der Lage, ihre Kunden über die Möglichkeiten der Förderung für IT-Sicherheitsmaßnahmen zu beraten. - Die IT-Dienstleister unterstützen ihre Kunden bei der Beantragung der Fördermaßnahmen. - Die Antragstellung wird für KMU erleichtert und eine Interessenskonvergenz mit dem IT-Dienstleister hergestellt.
Maßnahmen	- Befähigung der IT-Dienstleister in das notwendige Know-how für die Erbringung dieser Beratungsleistung - Unterstützung der IT-Dienstleister bei der Durchführung der Beratungsleistung durch staatlich Stellen, die IHKn oder Berufsverbände
Verweise	7.2.7, 7.2.8, 7.3.5, 7.3.6, 9.1.5.2, 9.2.7

10.5. Handlungsfeld 5: Qualität und Standards

Empfehlung 5.1	*Etablierung Gruppenzertifikaten für mehr IT-Sicherheit bei KMU*
Ziel	- Die Möglichkeit von Gruppenzertifizierungen und bereits existierender Services sollten für den Bereich IT-Sicherheit der KMU weiter etabliert und bekannt gemacht werden. - Reduktion von Aufwand und Kosten für KMU bei der Zertifizierung - Hinweis: Die Planung, Vorbereitung und das Erreichen von Zertifizierungen bedeutet für die Unternehmen immer Zeit- und Kostenaufwand. Wie auch bei Qualitätsmanagement-Zertifizierungen besteht im Bereich der Informationssicherheit die Möglichkeit, Gruppenzertifizierungen zu erhalten.
Maßnahmen	- Unterstützung der weiteren Etablierung von Gruppenzertifizierungen im Rahmen von Informationssicherheit und von IT-Sicherheitsstandards (ISO 27001) für KMU - Vernetzung von Unternehmen, die vergleichbare Unternehmensausrichtungen haben und mit Partnern vergleichbare IT-Sicherheitsmaßnahmen, -prozesse und Zertifizierungen anstreben - Entwicklung von normenkonformen Bausteinen für Gruppenzertifizierungen (IT-Strategie, Organisation von IT-Sicherheit, Checks, Richtlinien und Konzepte für IT-Sicherheit, Audits und Prüfungen) - Unterstützung der KMU bei der Integration der erforderlichen Prozesse - Nutzung von Synergieeffekten und weitere Vernetzung von Kooperationsplattformen mit den Zertifizierungsservices - Prüfungen und Audits können anschließend gemeinsam in der Gruppe erfolgen.
Verweise	7.2.3, 7.2.8, 9.1.5.2, 9.2.3, 9.2.5, 9.3.3

Empfehlung 5.2	*Erarbeitung von Qualitätskriterien und -standards für vertrauenswürdige IT-Dienstleister und IT-Sicherheitsdienstleistungen für KMU sowie Erstellung und bessere Verlinkung von Anbieterverzeichnissen*
Ziel	- Die Suche der KMU nach geeigneten Dienstleistern und Serviceangeboten für mehr IT-Sicherheit soll erleichtert werden. - Angebote und Suche nach geeigneten Dienstleistern, die nach den definierten Qualitätskriterien arbeiten, wird erleichtert.
Maßnahmen	- Prüfung bereits existierenden Standards (z.B. BSI-GS, ISO 27001, VdS 10000, IDW PS) und auch Personenzertifizierungen - Analyse der Hemmnisse zur weiteren Verbreitung der existierenden Angebote - Schaffung von Anbieterverzeichnissen mit definierten und nachprüfbaren Qualitätskriterien, um Suchkosten zu senken und Qualität zu erhöhen. - Transparente Darstellung und weitere Vernetzung von Sachverständigen und Personenregistern zu IT-Sicherheit
Verweise	7.3.3, 7.3.4, 9.1.5.2, 9.2.6, 9.2.8, 9.3.1

Empfehlung 5.3	*Bestehende Grundsätze und Standards für sichere IT-Systeme müssen verstärkt den IT-Dienstleistern als Intermediäre zum KMU vermittelt werden*
Ziel	- Die Bekanntheit von existierenden Branchengrundsätzen und Standards müssen verstärkt werden und bei den IT-Dienstleistern zur Anwendung kommen (z.B. BSI, Recplast; ZdH mit Routenplaner, usw.).
Maßnahmen	- Verstärkte Informationen und Verteilung von Leitfäden und KMU-Standards über die bestehenden Anlaufstellen und Netzwerke der IT-Dienstleister - Bessere Informationsverteilung zum Stand der Technik (vgl. Teletrust)
Verweise	7.2.3, 7.2.8, 7.3.3, 9.2.2

Empfehlung 5.4	*Stärkung von klar definierten Serviceangeboten und -paketen durch IT-Dienstleister für KMU*
Ziel	- Komplette Servicepakete und Serviceplattformen sollen KMU bei der Steigerung des IT-Sicherheitsniveaus unterstützen. - Die Servicepakete sollten nicht nur als individuelle Beratungen angeboten werden, sondern auch im Sinne der Übernahme und des Managens von IT-Servicepaketen für Infrastrukturen, Software, Plattformen sowie IT-Sicherheit verstanden werden.
Maßnahmen	- Analyse bereits existierender Serviceangebote für mehr IT-Sicherheit für KMU nach Technologien, Qualitätskriterien, Service- und Preismodellen - Klärung der Hemmnisse bei der weiteren Etablierung dieser Managed IT-Services - Vernetzung von Serviceanbietern mit IT-Dienstleistern für die Kundengruppe der KMU - Vernetzung von IT-Serviceanbietern mit Netzwerken und Transferstellen
Verweise	7.1.2, 7.2.3, 9.1.5.2, 9.2.2, 9.2.3, 9.2.5, 9.3.1, 9.3.4

10.6. Querschnittsthemen

Empfehlung 6.1	*Programmleitung und Projektmanagement Office (PMO)*
Ziel	- Steuerung und agile Weiterentwicklung der Maßnahmen - Förderung des Informationsaustauschs und Wissenstransfers
Maßnahmen	- Etablierung einer zentralen Programmleitung - Regelmäßige Überprüfung und Aktualisierung der Handlungsempfehlungen mit agiler Umsetzung - Informationsaustausch und Vernetzungsmaßnahmen mit den beteiligten Akteuren
Verweise	7.2.6

Empfehlung 6.2	*Jährliche Fachveranstaltung zu der Rolle der IT-Dienstleister für mehr Sicherheit bei KMU*
Ziel	- Zielgruppe: kleine und mittelgroße IT-Dienstleister, KMU mit eigener IT-Abteilung - Wissenstransfer und Aufbau von Netzwerkstrukturen - Fortführung der Strategie aus dieser Studie - Erhöhung des Sicherheitsniveaus bei KMU
Maßnahmen	- Durchführung einer jährlichen Konferenz für IT-Dienstleister zu deren Rolle für mehr Sicherheit bei KMU - Informationen über Bedrohung (z.B. BSI, IT-Sicherheitsunternehmen), Versicherungsmöglichkeiten, technische und organisatorische Schutzleistungen - Regelmäßige Überprüfung und Aktualisierung der Handlungsempfehlungen - Erhalten von aktuellen Lagebildern und Bedrohungslagen - Vernetzungsmaßnahmen von IT-Dienstleister für mehr Sicherheit bei KMU
Verweise	7.2.6, 7.3.6, 9.2.7, 9.2.8

11. Anhang

11.1. Abbildungsverzeichnis

11.2. Tabellenverzeichnis

11.3. Studien

- Accenture & Ponemon Institute LLC. (2019), The Cost of Cybercrime, Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Protection. Accenture.
- BDI [Bundesverband der Deutschen Industrie e.V.] (2017), Cybersicherheit in Deutschland und Europa, Berlin.
- Bitkom [Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.] (2016), Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie, Bitkom e. V., Berlin.
- Bitkom (2018), Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie, Bitkom e. V., Berlin. Studienbericht und Report.
- Bitkom & EITO (2019), ITK - Marktzahlen, Berlin.
- Bitkom (2019), Wirtschaftsschutz in der digitalen Welt, Berlin.
- Bitkom (2020a), Der IT-Mittelstand in Deutschland – IT-Mittelstandsbericht 2020, Berlin.
- Bitkom (2020b), Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt, Berlin.
- BKA [Bundeskriminalamt] (2019), Cybercrime. Bundeslagebild 2018, Wiesbaden.
- BKA (2020), Cybercrime. Bundeslagebild 2019, Wiesbaden.
- BMWi [Bundesministerium für Wirtschaft und Energie] (2016), IT-Sicherheit für Industrie 4.0 – Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten, Abschlussbericht, Berlin.
- BMWi (2019a), Wirtschaftsmotor Mittelstand Zahlen und Fakten zu den deutschen KMU, Berlin.
- BMWi (2019b), Von der Idee zum Markterfolg: Programme für einen innovativen Mittelstand, Berlin.
- Bretschneider, W.; Rieckmann, J.; Stuchtey, T.; Szanto, A. (2020), Cyber-Sicherheit als Katalysator für Innovation und Wachstum, Studien zum deutschen Innovationssystem 10-2020, Berlin: EFI.

- BSI [Bundesamt für Sicherheit in der Informationstechnik] (2011), Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen – Grad der Sensibilisierung des Mittelstands in Deutschland, Bonn.
- BSI (2017a), Cyber-Sicherheits-Umfrage 2017 – Cyber-Risiken, Meinungen und Maßnahmen, Bonn.
- BSI (2017b), Die Lage der IT-Sicherheit in Deutschland 2017, Bonn.
- BSI (2019a), Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen in Unternehmen, Betrachtungszeitraum 2018, Bonn.
- BSI (2019b), Die Lage der IT-Sicherheit in Deutschland 2019, Bonn.
- BSI (2020), Die Lage der IT-Sicherheit in Deutschland 2020, Bonn.
- Capgemini (2019), Intelligente Technologien – Vorreiter erzielen bereits Ergebnisse, Studie IT-Trends 2019, Berlin.
- Chubb (2018), Australia SME Cyber Preparedness Report.
- Cisco (2018), Cisco Cybersecurity Report 2018 SME Report, Small and Mighty.
- CrowdStrike (2018), Securing the Supply Chain, VansonBourne, Newbury.
- Cybersecurity Ventures (2020), 2019 Official Annual Cybercrime Report, Sponsored by Herjavec Group, Toronto, Canada.
- Deutschland sicher im Netz e.V. (2018), Praxisreport 2018 Mittelstand @IT-Sicherheit, Berlin.
- Deutschland sicher im Netz e.V. (2020), Praxisreport 2020 Mittelstand @IT-Sicherheit, Berlin.
- GDV [Gesamtverband der Deutschen Versicherungswirtschaft e. V.] (2018), Cyberrisiken im Mittelstand, Ergebnisse einer Forsa-Befragung, Berlin.
- Frost & Sullivan (2017), 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, Center for Cyber Safety and Education, ISC.
- Hochschule Düsseldorf (2018), Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU), Fachbereich Medien, Düsseldorf.

- IDG Business Media (2018), Systemhausstudien 2018 – Die besten Systemhäuser, München.
- it-sa Benefiz (2014), IT-Dienstleister und IT-Sicherheit in KMU – Fakten, Perspektiven, Handlungsoptionen, Lehrstuhl Wirtschaftsinformatik I – Informationssysteme, Universität Regensburg.
- KfW [Kreditanstalt für Wiederaufbau], Digitalisierungsbericht Mittelstand 2018, Digitalisierung erfasst breite Teile des Mittelstands – Digitalisierungsausgaben bleiben niedrig, Frankfurt am Main.
- KfN [Kriminologisches Forschungsinstitut Hannover e.V.] (2020), Cyberangriffe gegen Unternehmen. Ergebnisse einer repräsentativen Unternehmensbefragung in Deutschland 2018/2019, Hannover.
- Lünendonk (2019), Der Markt für IT-Beratung und IT-Service in Deutschland – Marktstruktur, Trends & Entwicklung aus Sicht von IT-Dienstleistern und Anwenderunternehmen, Mindelheim.
- McAfee (2018), The Economic Impact of Cybercrime: No Slowing Down. Center for Strategic and International Studies.
- Pierre Audoin Consultants (2013), Competitive Analysis of the UK Cyber Security Sector, London.
- Pierre Audoin Consultants & Fraunhofer ISI. (2012). Analyse von Wachstumshemmnissen kleiner und mittlerer Unternehmen am Beispiel der IT-Branche. München.
- Rieckmann, J., & Stuchtey, T. (2018). Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung. In G. Calaminus (Hg.), Kompendium Sicherheit – Gesellschaft – Digitalisierung von TCC Verlagsgesellschaft, S. 43-68.
- Senseon (2019), The State of Cybersecurity 2019 SME Report, London.
- Symantec (2016), Internet Security Threat Report, Mountain View, California, USA.
- Symantec (2019a), Internet Security Threat Report, Mountain View, California, USA.
- Symantec (2019b), Alarmstufe Rot: Wenn Cybersecurity aus dem Ruder läuft - Warum zusammengestückelte Insellösungen ein Problem sind und wie sie die Komplexität nachhaltig reduzieren, Mountain View, California, USA.
- Thales (2018), Data Threat Report - Trends in Encryption and Data Security, Paris.

- TÜV [Technischer Überwachungsverein] (2019), Cybersecurity Studie, Berlin.
- WiFOR Institut (2019), Der IT-Sicherheitsmarkt in Deutschland, Berlin.
- Wik [Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste] (2017), Aktuelle Lage der IT-Sicherheit in KMU, Bad Honnef.

11.4. Sonstige Dokumente

- Destatis (2019), Strukturerhebung im Dienstleistungsbereich Information und Kommunikation, Fachserie 9 Reihe 4.2, Statistisches Bundesamt, Wiesbaden.
- DQS [Deutsche Gesellschaft zur Zertifizierung von Managementsystemen] (2019), Weltweite Zertifizierungen und Begutachtungen aus einer Hand, Frankfurt am Main.
- TeleTrust (2019), IT-Sicherheitsgesetz und Datenschutz-Grundverordnung – Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen, Berlin.
- VdS (2015), Cyber-Security für kleine und mittlere Unternehmen (KMU), Köln.

11.5. Begleitschreiben des Bundesministeriums für Wirtschaft und Energie für die qualitative Befragung der IT-Dienstleister

Bundesministerium für Wirtschaft und Energie

Bundesministerium für Wirtschaft und Energie 11019 Berlin

Frank Fischer
Referatsleiter Mittelstand - Digital

TEL +49 30 18615 6230
E-MAIL frank.fischer@bmwi.bund.de
INTERNET www.bmwi.de

Berlin, 19. Februar 2020

IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU

Sehr geehrte Damen und Herren,

das **Bundesministerium für Wirtschaft und Energie** hat im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ eine Studie zum Thema „IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU“ vergeben. Im Rahmen der Studie sollen in einem ersten Schritt rund 25 deutsche IT-Dienstleister als kleine systematische Stichprobe ausgewählt und in qualitativen Interviews befragt werden.

Sie sind eines der ausgewählten Unternehmen. Wir ersuchen Ihre Unterstützung und bitten um die Teilnahme an dieser Befragung.

Die Befragung wird von der NKMG | Neue Köhler Managementgesellschaft mbH durchgeführt.

Ziel der Befragung ist es, bisher fehlendes, näheres Wissen zu IT-Dienstleistern, ihrer Leistungserbringung für KMU in der Digitalisierung und der Verbesserung der IT-Sicherheit zu gewinnen.

Ihre Teilnahme an der Befragung liefert einen wichtigen Beitrag für ein besseres Verständnis der Branche der IT-Dienstleister unter Berücksichtigung der IT-Sicherheit in Deutschland.

Die Befragung erfolgt nach wissenschaftlichen Standards, die Befragungszeit beträgt rund 45 Minuten. Dazu wird ein/e Mitarbeiter/in von der NKMG telefonisch mit Ihnen Kontakt aufnehmen. Ihre Antworten werden nur anonym und in aggregierter Form ausgewertet. Es sind keine Rückschlüsse auf Ihr Unternehmen möglich.

Auf Wunsch erhalten Sie gerne die Ergebnisse der Untersuchungen.

Falls Sie sich weiter über die Initiative „IT-Sicherheit in der Wirtschaft“ informieren wollen, besuchen Sie uns unter **http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/meldungen.html.**
Für inhaltliche Fragen steht Ihnen Charmaine Rickerson, Leiterin dieser Studie (Tel.:+49 177 59 40 551; E-Mail: charmaine.rickerson@nkmg-berlin.de), gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Frank Fischer
Referatsleiter Mittelstand - Digital

HAUSANSCHRIFT Scharnhorststraße 34 - 37
10115 Berlin
VERKEHRSANBINDUNG U6 Naturkundemuseum
S-Bahn Berlin Hauptbahnhof
Tram Invalidenpark

11.6. Begleitschreiben des Bundesministeriums für Wirtschaft und Energie für die quantitative Befragung der IT-Dienstleister

Bundesministerium
für Wirtschaft
und Energie

Bundesministerium für Wirtschaft und Energie • 11019 Berlin

Frank Fischer
Referatsleiter Mittelstand - Digital

TEL +49 30 18615 6230
E-MAIL frank.fischer@bmwi.bund.de
INTERNET www.bmwi.de

Berlin, im April 2020

IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU

Sehr geehrte Damen und Herren,
das Bundesministerium für Wirtschaft und Energie hat eine Studie zum Thema **„IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU“** in Auftrag gegeben.
Im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ wird das Projekt eine **Online-Umfrage** durchführen und IT-Dienstleister zu IT-Sicherheitsthemen in der Kundengruppe der KMU befragen.

Ziel ist es, Kenntnisse über die Leistungserbringung durch IT-Dienstleister für KMU in der Digitalisierung und der IT-Sicherheit zu gewinnen. Aus den Ergebnissen der Umfrage lassen sich fundierte Analysen erstellen und Handlungsempfehlungen ableiten.
Ich würde mich freuen, wenn Sie das Projekt durch die Beantwortung des Fragebogens unterstützen würden. Ihre Teilnahme liefert einen wichtigen Beitrag für ein besseres Verständnis der Branche der IT-Dienstleister in Deutschland.

Die Beantwortungszeit des Fragebogens beträgt rund **15 Minuten**. Die Befragung erfolgt nach wissenschaftlichen Standards. Ihre Antworten werden nur **anonym** und in aggregierter Form ausgewertet. Auf Wunsch werden Ihnen die Ergebnisse der Untersuchungen zur Verfügung gestellt.

Die Befragung wird von der Neue Köhler Managementgesellschaft mbH (NKMG) gemeinsam mit dem Brandenburgischen Institut für Gesellschaft und Sicherheit gGmbH (BIGS) durchgeführt.
Wissenschaftliche Unterstützung bei der Befragung erhält das Vorhaben durch die Hochschule für Technik und Wirtschaft Berlin (HTW).

Für allgemeine Informationen besuchen Sie die Homepage der Initiative „IT-Sicherheit in der Wirtschaft“ unter https://www.it-sicherheit-in-der-wirtschaft.de.

Für inhaltliche Fragen steht Ihnen die Leiterin der Studie Charmaine Rickerson (+49 177 59 40 551, charmaine.rickerson@nkmg-berlin.de) zur Verfügung.

Teilnahme-Link: https://www.soscisurvey.de/BefragungITDienstleister/.

Mit freundlichen Grüßen

i.A. Frank Fischer
Referatsleiter Mittelstand - Digital

HAUSANSCHRIFT Scharnhorststraße 34 - 37
10115 Berlin
VERKEHRSANBINDUNG U6 Naturkundemuseum
S-Bahn Berlin Hauptbahnhof
Tram Invalidenpark

11.7. Begleitschreiben des Bundesministeriums für Wirtschaft und Energie für die quantitative Befragung der KMU

Bundesministerium für Wirtschaft und Energie

Bundesministerium für Wirtschaft und Energie □11019 Berlin

Frank Fischer
Referatsleiter Mittelstand - Digital

TEL +49 30 18615 6213
E-MAIL Buero-AstMi3@bmwi.bund.de
INTERNET www.bmwi.de

Berlin, im Juli 2020

KMU als Nachfrager von IT-Dienstleistungen für mehr IT-Sicherheit bei KMU

Sehr geehrte Damen und Herren,

das **Bundesministerium für Wirtschaft und Energie** hat im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft“ eine Studie zum Thema „IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU“ vergeben. Im Rahmen des Projektes werden kleinere und mittlere Unternehmen (KMU) als Nachfrager nach IT-Sicherheitsdienstleistungen anhand einer strukturierten Online-Befragung zu Ihren Anforderungen, der Auswahl sowie der Zusammenarbeit mit IT-Dienstleistern befragt.

Die Befragung wird von der NKMG | Neue Köhler Managementgesellschaft mbH gemeinsam mit dem BIGS | Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (BIGS) durchgeführt. Wissenschaftliche Unterstützung bei der Befragung erhält das Vorhaben durch die Hochschule für Technik und Wirtschaft (HTW) Berlin.

Ziel der Befragung ist es, bisher fehlendes Wissen zu den Anforderungen der KMU bei der Suche und der Auswahl von IT-Dienstleistern für mehr IT-Sicherheit im eigenen Unternehmen (KMU) zu gewinnen.

Ich würde mich freuen, wenn Sie das Projekt durch die Beantwortung des Fragebogens unterstützen würden. Sie helfen uns damit, fundierte Analysen und Handlungsempfehlungen aus dem Projekt ziehen zu können.

Ihre Teilnahme an der Befragung liefert einen wichtigen Beitrag für ein besseres Verständnis der Anforderungen der KMU an die Auswahl der IT-Dienstleister unter Berücksichtigung der IT-Sicherheit.

Die Befragung erfolgt nach wissenschaftlichen Standards. Die Beantwortungszeit des Fragebogens beträgt rund 20 Minuten. Ihre Antworten werden nur anonym und in aggregierter Form ausgewertet. Es sind keine Rückschlüsse auf Ihr Unternehmen möglich.

Auf Wunsch bekommen Sie gern die Ergebnisse der Untersuchungen.

Falls Sie sich weiter über dieses Projekt und die Initiative „IT-Sicherheit in der Wirtschaft“ informieren wollen, besuchen Sie uns gern unter **https://www.it-sicherheit-in-der-wirtschaft.de** . Für inhaltliche Fragen steht Ihnen Christian Köhler, Geschäftsführer NKMG mbH (E-Mail: christian.koehler@nkmg-berlin.de), gerne zur Verfügung.

Hier der Link zur Befragung: https://www.soscisurvey.de/KMUITSIC/.

Mit freundlichen Grüßen
Im Auftrag

Frank Fischer
Referatsleiter Mittelstand - Digital

HAUSANSCHRIFT Scharnhorststraße 34 - 37
10115 Berlin
VERKEHRSANBINDUNG U6 Naturkundemuseum
S-Bahn Berlin Hauptbahnhof
Tram Invalidenpark

12. Literaturverzeichnis

Accenture & Ponemon Institute LLC. (2019). *The Cost of Cybercrime. NINTH ANNUAL COST OF CYBER-CRIME STUDY UNLOCKING THE VALUE OF IMPROVED CYBERSECURITY PROTECTION.* Accenture.

Anderson, R. (2001). Why Information Security is hard: An economic perspective. *Seventeenth Annual Computer Security Applications Conference. IEEE, 2001.*

Bitkom & EITO. (2019). *IKT-Marktzahlen.* Berlin.

Bitkom. (2018a). *Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie.* Berlin: Studienbericht.

Bitkom. (2018b). *Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie.* Berlin: Report.

Bitkom. (2019). *Wirtschaftsschutz in der digitalen Welt.* Berlin.

Bitkom. (2020a). *Der IT-Mittelstand in Deutschland – IT-Mittelstandsbericht 2020.* Berlin.

Bitkom. (2020b). *Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der vernetzten Welt.* Berlin.

BKA. (2020). *Cybercrime Bundeslagebild 2019.* Wiesbaden: Bundeskriminalamt.

BMWI. (2019a). *Wirtschaftsmotor Mittelstand Zahlen und Fakten zu den deutschen KMU.* Berlin.

BMWI. (2019b). *Von der Idee zum Markterfolg: Programme für einen innovativen Mittelstand.* Berlin.

Bretschneider, W., Riekmann, J., Stuchtey, T., & Szanto, A. (2020). Cyber-Sicherheit als Katalysator für Innovation und Wachstum. *Studien zum deutschen Innovationssystem 10-2020, Berlin: EFI*.

Bretschneider, W., Freytag, A., Rieckmann, J., & Stuchtey, T. (2020). Sicherheitsverantwortung zwischen Staat und Markt – eine institutionenökonomische Analyse. ORDO Band 70: Heft 1, S. 89-144. Berlin.

BSI. (2011). *Die Lage der IT-Sicherherheit in Deutschland.* Bonn.

BSI. (2017a). *Cyber-Sicherheits-Umfrage 2017.* Bonn: Allianz für Cybersicherheit.

BSI. (2017b). *Die Lage der IT-Sicherheit in Deutschland.* Bonn.

BSI. (2019a). *Cyber-Sicherheits-Umfrage - Cyber-Risiken & Schutzmaßnahmen in Unternehmen.* Bonn: Betrachtungszeitraum 2018.

BSI. (2019b). *Die Lage der IT-Sicherheit in Deutschland 2019.* Bonn.

BSI. (2020). *Die Lage der IT-Sicherheit in Deutschland 2020.* Bonn.

Bundesverband der deutschen Industrie (BDI). (2017). *Cybersicherheit in Deutschland und Europa.* Berlin.

Capgemini. (2019). *Studie IT-Trends 2019 Intelligente Technologien.* Berlin: Capgemini Deutschland 2019.

Crowdstrike. (2018). *Securing the Supply Chain.* Newbury: VansonBourne.

Cybersecurity Ventures. (2019). *Official Annual Cybercrime Report.* Toronto, Canada: Sponsored by Herjavec Group.

Destatis. (2008). *Gliederung der Klassifikation der Wirtschaftszweige*: Statistisches Bundesamt.

Destatis. (2019). *Strukturerhebung im Dienstleistungsbereich Information und Kommunikation.* Fachserie 9 Reihe 4.2: Statistisches Bundesamt.

DsiN Deutschland sicher im Netz e.V. (2018). *Praxisreport 2018 Mittelstand @IT-Sicherheit.* Berlin.

Deutschland sicher im Netz e.V. (2020). *Praxisreport 2020 Mittelstand @IT-Sicherheit.* Berlin.

DQS. (2019). *Weltweite Zertifizierungen und Begutachtungen aus einer Hand.* Frankfurt am Main.

Fritsch, M. (2018). *Marktversagen und Wirtschaftspolitik. Mikroökonomische Grundlagen staatlichen Handelns.* München, 10. A: Vahlen.

Frost & Sullivan. (2017). *Global Information Security Workforce Study: Benchamrking Workforce Capacity and Response to Cyber Risk.* Center for Safety and Education, ISC.

GDV (Gesamtverband der Deutschen Versicherungswirtschaft). (2018). *Cyberrisiken im Mittelstand.* Berlin.

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018). *Cyberrisiken im Mittelstand.* Berlin.

IDG. (2018). *Security Priorities Study - Exploring security roles and technologies that keep the enterprise functioning.* Boston.

IDG Business Media GmbH. (2018). *Systemhausstudie 2018.* München.

it-sa Benefiz. (2014). *IT-Dienstleister und IT-Sicherheit in KMU.* it-sa Benefiz - Gemeinnütziger Verein zur Förderung der IT-Sicherheit e.V. und Lehrstuhl Wirtschaftsinformatik I – Informationssysteme (Prof. Dr. Günther Pernul) Universität Regensburg.

KfW. (2018). *Digitalisierungsbericht Mittelstand 2018.* Frankfurt am Main: KfW Research.

Lünendonk. (2019). *Der Markt für IT-Beratung und IT-Service in Deutschland.* Mindelheim: Lünendonk & Hossenfelder GmbH.

McAfee. (2018). *The Economic Impact of Cybercrime: No Slowing Down. Center for Strategic and International Studies. & Hackmageddon – Cyber Attacks Statistics.* Von https://www.hackmageddon.com/category/security/cyber-attacks-statistics abgerufen

Mijnhardt, F., Baars, T., & Spruit, M. (2016). Organizational Characteristics Influencing SME. *Journal of Computer Information Systems*, S. 106-115.

Moore, T. (3.3-4 2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, S. 103-117.

Moore, T. D. (2015). Identifying how firms manage cybersecurity investment. *Southern Methodist University.*

Park, J.-Y., Robles, R., Hong, C.-H., Yeo, S.-S., & Kim, T.-h. (Vol. 2, No. 3, July 2008). IT Security Strategies for SME's. *International Journal of Software Engineering and Its Applications*, S. 91-98.

Pierre Audoin Consultants & Fraunhofer ISI. (2012). *Analyse von Wachstumshemmnissen kleiner und mittlerer Unternehmen am Beispiel der IT-Branche.* München.

Riekmann , J., & Stuchtey , T. (2018). Die Vermessung der Sicherheitswirtschaft – Wachstum und Veränderung im Zeichen der Digitalisierung. *in G. Calaminus (Hg.), Kompendium Sicherheit – Gesellschaft – Digitalisierung von TCC Verlagsgesellschaft*, S. 43-68.

Schmitz, P. (2019). *Positiver Sicherheitstrend bei KMU für 2019*. Von www.security-insider.de: https://www.security-insider.de/positiver-sicherheitstrend-bei-kmu-fuer-2019-a-889695/[zuletzt abgerufen am 10.02.2020] abgerufen

Senseon. (2019). *The State of Cybersecurity 2019 SME Report.* London.

Statista. (2019). *Ausgaben für IT-Sicherheit in Deutschland nach Segment in den Jahren 2017 und 2018 und Prognose für 2019*. Von www.statista.com: https://de.statista.com/statistik/daten/studie/151727/umfrage/ausgaben-fuer-it-sicherheit-in-deutschland/[abgerufem am 27.02.20] abgerufen

Symantec. (2016). *Internet Security Threat Report.* Mountain View, California, USA.

Symantec. (2019a). *Internet Security Threat Report.* Mountain View, California, USA.

Symantec. (2019b). *Alarmstufe Rot: Wenn Cybersecurity aus dem Ruder läuft - Warum zusammengestückelte Insellösungen ein Problem sind und wie sie die Komplexität nachhaltig reduzieren.* Mountain View, California, USA.

Thales. (2018). *Data Threat Report – Trends in Encryption and Data Security.* Paris.

TÜV. (2019). *Cybersecurity Studie.* Berlin.

WiFOR Institute. (2019). *Der IT-Sicherheitsmarkt in Deutschland.* Berlin, Darmstadt.

wik (Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste. (2017). *Aktuelle Lage der IT-Sicherheit in KMU.* Bad Honnef.