KfW Research
Fokus Volkswirtschaft

Cyberkriminalität bedroht vor allem die Vorreiter der Digitalisierung

Nr. 419, 23. Februar 2023

Autor: Dr. Volker Zimmermann, Telefon 069 7431-3725, volker.zimmermann@kfw.de

29 % der mittelständischen Unternehmen sind im Zeitraum von 2018–2020 Opfer von Cyberkriminalität geworden. Betroffen davon sind vor allem große Mittelständler (49 % der Unternehmen mit 100 oder mehr Beschäftigten) und Unternehmen mit ausgeprägten Digitalisierungsaktivitäten. Dies gilt etwa hinsichtlich der Höhe der Ausgaben für die Digitalisierung (43 % der Unternehmen mit Digitalisierungsausgaben von 10.000 EUR oder mehr), der Bandbreite der verschiedenen Digitalisierungsprojekte (45 % der Unternehmen mit 4 oder mehr verschiedenen Projektarten) und für Unternehmen mit einer Digitalisierungsstrategie (37 %).

Wesentlicher Grund für die häufigere Betroffenheit von Vorreitern ist die größere Angriffsfläche dieser Unternehmen in Verbindung mit unzureichenden Schutzvorkehrungen. Die Anstrengungen zur Verbesserung der IT-Sicherheit müssen daher dringend erhöht werden. Dies gilt nicht nur für die Vorreiter, sondern auch für die kleinen und nur in einem geringen Umfang digital aktiven Unternehmen. Denn diese Unternehmen sind mit Anteilen von rund einem Viertel ebenfalls häufig Opfer von Cyberkriminalität.

Schutzvorkehrungen werden gerade in mittelständischen Unternehmen häufig nicht getroffen, da in vielen Unternehmen das fachliche Knowhow fehlt. Die Bedrohungslage wird oftmals nicht erkannt und notwendige Investitionen in die IT-Sicherheit unterbleiben.

Daher gilt es, die Unternehmen für die Bedrohung durch Internetkriminalität zu sensibilisieren und zum Aufbau von Knowhow hinsichtlich IT-Sicherheit anzuregen. Dazu können für die Unternehmen attraktive Schulungsangebote und – soweit verfüg- und bezahlbar – auch die Einstellung von IT-Experten beitragen. Auch eine Auslagerung der IT-Sicherheit an spezialisierte IT-Dienstleister kann eine Lösung sein. Dazu wäre es hilfreich, das Angebot und die Transparenz darüber gerade für kleine und mittlere Unternehmen zu erhöhen. Nicht zuletzt kann die weitere Etablierung spezifischer IT-Sicherheitsstandards- und -zertifizierungen dabei helfen, die IT-Sicherheit und das Bewusstsein der Beschäftigten zum Umgang mit Informationstechnik schärfen.

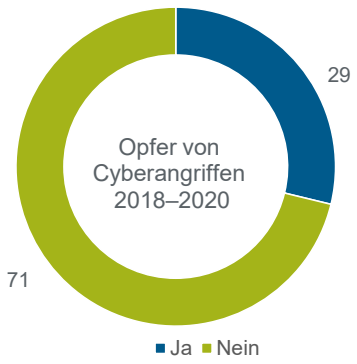
Die Digitalisierung hat sich in Deutschland aktuell noch nicht zu einem Selbstläufer entwickelt. Die Investitionen in die digitale Transformation fallen deutlich hinter jene von vergleichbaren Ländern zurück.[1] Vor allem kleine und mittlere Unternehmen weisen niedrige Digitalisierungsaktivitäten auf. Dennoch kann hinsichtlich der Digitalisierung die positive Nachricht hervorgehoben werden, dass zunehmend mehr Unternehmen die Bedeutung der Digitalisierung auch für ihre Organisation erkennen. So kann beobachtet werden, dass auf mittlere Frist der Anteil der Unternehmen mit Digitalisierungsaktivitäten zunimmt.[2] Auch gehen zunehmend mehr Unternehmen ihre Digitalisierung unter strategischen Gesichtspunkten an.[3] Zuletzt dürften insbesondere die Erfahrungen der Corona-Pandemie vielen Unternehmen vor Augen geführt haben, wie wichtig die Digitalisierung ist, um auch zukünftig Kunden an sich zu binden.[4]

Zunehmende Bedrohung durch Internetkriminalität

Die zunehmende Digitalisierung der Unternehmen öffnet jedoch auch die Tür für eine neue Art der Bedrohung. Sie macht die Unternehmen zunehmend gegenüber Internetkriminalität verletzlich. Mögliche Gefahren entstehen bei der Nutzung einer Vielzahl von digitalen Technologien. Sie reichen vom zunehmenden digitalen Informations- und Datenaustausch, über die Nutzung von E-Commerce und Social Media, bis hin zur Vernetzung der Produktion oder zur unternehmensübergreifenden Projektarbeit. Cyberangriffe sind daher seit geraumer Zeit eine permanente Gefahr für Unternehmen. Entsprechende Warnungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) bestehen seit Jahren. Aktuell wird zusätzlich vor einer erhöhten Gefahrenlage in der Folge des Angriffskriegs Russlands auf die Ukraine gewarnt.[5]

Grafik 1: Betroffenheit von Cyberangriffen im Mittelstand

Anteile in Prozent



Quelle: KfW-Mittelstandspanel 2021, eigene Berechnung.

Vor diesem Hintergrund untersucht die vorliegende Studie die Betroffenheit mittelständischer Unternehmen von Cyberangriffen. Dazu wurde erstmalig in einer Haupterhebung des KfW-Mittelstandspanels erfragt, ob mittelständische Unternehmen in den Jahren 2018–2020 Opfer von Cyberangriffen geworden sind. Die vorliegende Studie setzt somit die bereits vor Jahren

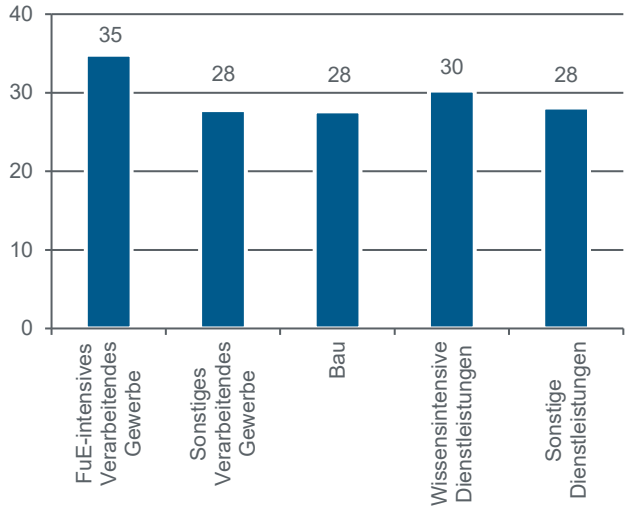
aufgenommene Berichterstattung zu IT-Sicherheit im Mittelstand fort.[6]

3 von 10 Mittelständler sind Opfer von Cyberangriffen

Im Untersuchungszeitraum sind 29 % der mittelständischen Unternehmen Opfer von Cyberattacken geworden (Grafik 1). Die Hauptbedrohung geht von der Erpressung von Löse- oder Schweigegeld aus. Dabei dringen Schadprogramme in die IT-Systeme der betroffenen Unternehmen ein und verschlüsseln oder entwenden vorhandene Daten. Für die Entschlüsselung der Daten verlangen die Angreifer Lösegeldzahlungen oder drohen, die erbeuteten, oftmals sensiblen Daten zu veröffentlichen. Eine weitere, sehr verbreitete Angriffsmethode ist die gezielte Überlastung von Internetseiten, die zu einer vorrübergehenden Unerreichbarkeit oder auch zu Systemabstürzen führt („Denial of Service-Angriffe“). Die Angriffe erfolgen dabei häufig auf sogenannte Perimeter-Systeme, wie Router und Firewalls, da solche Systeme oftmals weniger gut geschützt sind. Solche Angriffe können mit einem geringeren Aufwand erfolgen als etwa spezifische Angriffe mit in E-Mails versteckter Schadsoftware.[7]

Grafik 2: Betroffenheit von Cyberangriffen nach der Wirtschaftszweigzugehörigkeit 2018–2020

Anteile in Prozent



Quelle: KfW-Mittelstandspanel 2021, eigene Berechnung.

Alle Wirtschaftszweige von Cyberkriminalität betroffen

Der Blick auf die Wirtschaftszweige zeigt, dass alle Branchengruppen nahezu gleich häufig von Cyberangriffen betroffen sind (Grafik 2). Lediglich die Unternehmen aus den Wirtschaftszweigen der wissensbasierten Dienstleistungen[8] mit 30 % und jene des FuE-intensiven Verarbeitenden Gewerbes[9] mit 35 % sind etwas häufiger als die anderen Wirtschaftszweige Opfer von Angriffen. Auffällig hierbei ist, dass gerade Unternehmen dieser Wirtschaftszweige häufig auch Vorreiter bei der Digitalisierung sind.[10] Dieses Untersuchungsergebnis gibt einen ersten Hinweis darauf, dass vor allem Unternehmen, die digitale Technologien bereits in einem stärkeren Umfang nutzen, häufiger Opfer von Cyberkriminalität werden.

Große Mittelständer sind vermehrt Opfer von Cyberkriminalität

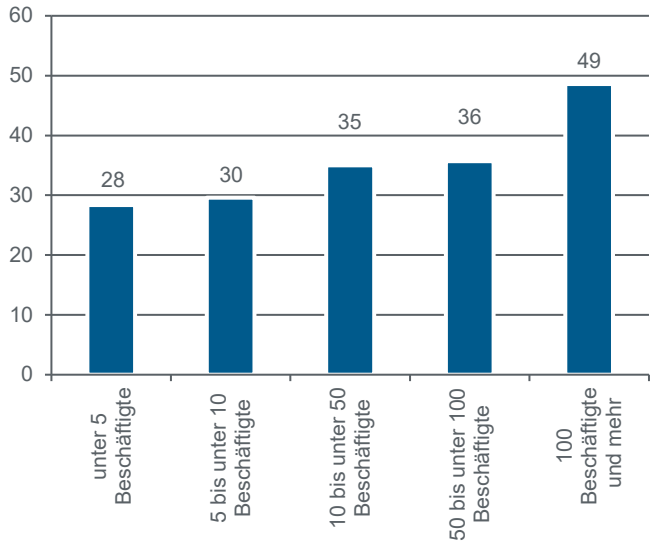
Dagegen zeigt sich zwischen der Unternehmensgröße und der Betroffenheit von Cyberkriminalität ein stark ausgeprägter Zusammenhang. Der Anteil der Opfer von Cyberkriminalität steigt von 28 % bei den kleinen Unternehmen (weniger als fünf Beschäftigte) bis auf 49 % bei den Unternehmen mit 100 und mehr Beschäftigten (Grafik 3). Ein Grund für die höhere Betroffenheit großer Mittelständler ist, dass Cyberkriminelle insbesondere für Erpressungsversuche vor allem umsatzstarke Unternehmen angreifen.[11] Da größere mittelständische Unternehmen ebenfalls häufiger zu den digitalen Vorreiterunternehmen zählen, liegt darüber hinaus die Vermutung nahe, dass der höhere Digitalisierungsgrad dieser Unternehmen in einem Zusammenhang mit ihrer häufigeren Betroffenheit von Cyberkriminalität steht.

Betroffenheit von Cyberkriminalität steigt mit der Breite und Intensivität der Digitalisierungsaktivitäten

Zum Zusammenhang zwischen der Betroffenheit von Cyberkriminalität und der Größe der Angriffsfläche, die ein Unternehmen bietet, sind in Grafik 4 Auswertungen zu verschiedenen Aspekten für die Breite und die Intensität der Digitalisierungsaktivitäten eines Unternehmens wiedergegeben.[12]

Grafik 3: Betroffenheit von Cyberangriffen nach der Unternehmensgröße 2018–2020

Anteile in Prozent

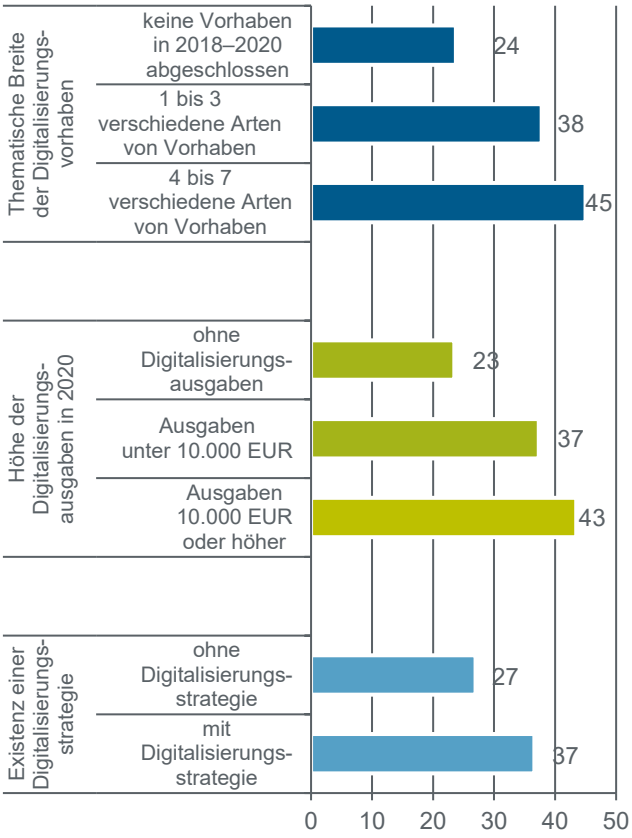


Quelle: KfW-Mittelstandspanel 2021, eigene Berechnung.

Die Untersuchung nach der thematischen Breite der durchgeführten Digitalisierungsvorhaben zeigt, dass vor allem Unternehmen, die viele verschiedene Arten von Vorhaben durchführen, häufiger Opfer von Cyberkriminalität sind. So liegt der Anteil der von Cyberkriminalität betroffenen Unternehmen, die 4 bis 7 verschiedene Vorhabensarten durchgeführt haben, bei 45 %. Bei den Unternehmen mit weniger Vorhabensarten beträgt er lediglich 38 % und bei Unternehmen ohne aktuell abgeschlossene Vorhaben sogar nur 24 %.

Grafik 4: Betroffenheit von Cyberangriffen nach dem Umfang der Digitalisierungsaktivitäten 2018–2020

Anteile in Prozent



Quelle: KfW-Mittelstandspanel 2021, eigene Berechnung.

Ähnliche Ergebnisse können auch hinsichtlich der Höhe der Digitalisierungsausgaben ermittelt werden. Unternehmen mit vergleichsweise umfangreichen Digitalisierungsausgaben (10.000 EUR und mehr) wurden im Untersuchungszeitraum mit einem Anteil von 43 % am häufigsten Opfer von Cyberkriminalität. Damit liegt der Anteil bei diesen Unternehmen um gut ein Siebtel bzw. um nahezu das Doppelte höher als bei den Unternehmen mit geringeren bzw. ohne Digitalisierungsausgaben im Jahr 2020.

Das Vorliegen einer Digitalisierungsstrategie in einem Unternehmen kann als Indikator für besonders ambitionierte Digitalisierungsaktivitäten herangezogen werden. Dies gilt nicht nur für die Breite der Aktivitäten und die Höhe der Digitalisierungsausgaben. Unternehmen mit Digitalisierungsstrategie wenden auch häufiger als andere Unternehmen anspruchsvolle Technologien (z. B. Künstliche Intelligenz oder Big Data-Anwendungen) an.[13] Wie Grafik 4 zeigt, sind Unternehmen mit Digitalisierungsstrategie mit 37 % gut ein Drittel häufiger Opfer von Cyberkriminalität als Unternehmen ohne eine Digitalisierungsstrategie.

Diese Ergebnisse zeigen deutlich, dass aktivere Unternehmen häufiger Opfer von Cyberkriminalität werden. Dies bestätigt Überlegungen, dass die Größe der Angriffsfläche, die ein Unternehmen für Cyberangriffe bietet, eine wesentliche Rolle spielt.[14]

Schutzmaßnahmen hinken oftmals der Angriffsfläche für Cyberattacken hinterher

Dass höher digitalisierte Unternehmen für mögliche Bedrohungen eine größere Angriffsfläche bieten, ist ein Aspekt zur Erklärung der Betroffenheit von Cyberkriminalität. Angriffe auf Unternehmen können jedoch nur dann erfolgreich sein, wenn in dem betreffenden Unternehmen nicht in einem ausreichenden Maße Schutzvorkehrungen zur Abwehr solcher Bedrohungen getroffen worden sind.

Dies ist insbesondere bei kleinen und mittleren Unternehmen häufig der Fall. Denn die Gewährleistung von IT-Sicherheit stellt besondere Anforderungen an die fachliche Qualifikation von Mitarbeitenden und Führungskräften. Insbesondere kleine und mittlere Unternehmen aber haben oftmals nicht das erforderliche Personal, um die Absicherung von IT-Systemen sicherzustellen.[15] Spezifische IT-Abteilungen existieren in diesen Unternehmen zumeist nicht. Zudem sind fehlende digitale Kompetenzen im Mittelstand ein generelles Problem, wie in verschiedenen Untersuchungen ermittelt werden konnte.[16] In vielen Unternehmen liegen daher keine oder lediglich rudimentäre Kenntnisse über die allgemeine Bedrohungslage hinsichtlich Cyberkriminalität und zum firmeneigenen Risikoprofil im Speziellen vor. Als Folge davon entwickeln viele Unternehmen kein Bewusstsein für die Notwendigkeit, in IT-Sicherheit zu investieren.

Falls Unternehmen die Bedrohungslage erkennen, ist es insbesondere für kleinere Unternehmen aufgrund des Fachkräftemangels bei IT-Experten – und der Knappheit von IT-Kenntnissen in der Erwerbsbevölkerung insgesamt – schwierig, entsprechendes Personal zu rekrutieren. Auch die Auslagerung an Dienstleister fällt oftmals nicht leicht, da es kleinen und mittleren Unternehmen schwerfällt, IT-Dienstleister mit entsprechender Expertise vorab zu identifizieren. Auch existieren aktuell noch zu wenige Dienstleister mit einer solchen Expertise. Dies hat zur Folge, dass diese Dienstleister zumeist volle Auftragsbücher haben, und kleinere Unternehmen, die lediglich ein begrenztes Auftragsvolumen, zugleich aber individuelle und nicht skalierbare Beratungs- und Leistungsbedarfe nachfragen, nur begrenzt attraktive Kunden für sie darstellen.[17] Investitionen in die IT-Sicherheit sind, egal auf welche Weise sie erfolgen, mit zusätzlichen Kosten für das betreffende Unternehmen verbunden. Ohne ein entsprechendes Bewusstsein für die Risiken sind viele Unternehmen daher nicht bereit, solche Kosten auf sich zunehmen.

Fazit

Mit rund 3 von 10 Unternehmen wurde in den Jahren 2018–2020 ein beachtlicher Anteil der mittelständischen Unternehmen Opfer von Cyberkriminalität. Betroffen davon sind vor allem größere und hinsichtlich der Digitalisierung aktivere Unternehmen. Jedoch auch unter den kleinen und weniger aktiven Unternehmen erreicht dieser Anteil mit Werten von rund einem Viertel eine beachtliche Höhe. Da aufgrund der zunehmenden Digitalisierung der Unternehmen auch die potenzielle Angriffsfläche für kriminelle Machenschaften steigt, ist zu befürchten, dass Cyberkriminalität in den kommenden Jahren noch weiter zunehmen wird.

Die Untersuchungsergebnisse offenbaren, dass die getroffenen Schutzvorkehrungen in vielen Unternehmen nicht adäquat zur Bedrohungslage durch Cyberkriminalität ausfallen. Verstärkte Anstrengungen müssen unternommen werden, um die

IT-Sicherheit zu erhöhen. Als Grund für den unzureichenden Schutz vor Cyberangriffen gilt insbesondere, dass in den Unternehmen häufig fachliches Knowhow fehlt. Die Bedrohungslage wird in vielen Unternehmen daher nicht erkannt und notwendige Investitionen in die IT-Sicherheit unterbleiben.

Daher erscheint es zwingend notwendig, vor allem kleine und mittlere Unternehmen für die Bedrohung von Internetkriminalität zu sensibilisieren sowie in diesen Unternehmen Knowhow hinsichtlich der IT-Sicherheit aufzubauen.[18] Eine Erhöhung der Transparenz hinsichtlich der Bedrohungslage, etwa durch Bündelung bestehender Informationsplattformen, könnte ein Weg sein, das Bewusstsein für die Bedrohungslage zu schärfen. Weiterbildungsmaßnahmen oder auch die Einstellung von IT-Experten können das benötigte Knowhow im Unternehmen steigern. Viele IT-Sicherheitsvorfälle ließen sich mit entsprechenden IT-Sicherheitsschulungen, Trainings und regelmäßigen Auffrischungskursen vermeiden. Die Verbesserung des IT-sicherheitsrelevanten Wissens in Unternehmen trägt nicht nur zu einem höheren Schutz vor Cyberkriminalität bei. Da Unsicherheit über die Anforderungen bei Datensicherheit und -schutz mit zu den am häufigsten genannten Digitalisierungshemmnissen zählen,[19] kann auch vermutet werden, dass ein verbesserter Kenntnisstand diesbezüglich zu einer Steigerung der Digitalisierungsanstrengungen mittelständischer Unternehmen führen wird.

Auch die Inanspruchnahme von IT-Dienstleistern mit entsprechender Expertise kann die IT-Sicherheit in mittelständischen Unternehmen erhöhen. Solche Dienstleister sind jedoch oftmals nur schwierig zu identifizieren. Daher würde die Schaffung von Anbieterverzeichnissen mit definierten Qualitätskriterien, in denen auch Sachverständige zu IT-Sicherheit aufgelistet sind, zu einer höheren Transparenz und zu geringeren Suchkosten bei den betroffenen Unternehmen führen. Eine Verbreiterung der Anzahl der auf kleine und mittlere Unternehmen spezialisierten Anbieter würde helfen, die bereits bestehende Nachfrage nach IT-Sicherheitsexpertise gerade kleinerer Unternehmen besser zu decken. Nicht zuletzt kann die weitere Etablierung spezifischer IT-Sicherheitsstandards- und -zertifizierungen dabei helfen, die IT-Sicherheit zu optimieren und das Bewusstsein der Beschäftigten zu einem professionellen Umgang mit der Informationstechnik und mit schützenswerten Daten zu erhöhen.

---

[1] Vgl. Zimmermann, V. (2021): Digitalisierung im internationalen Vergleich: Deutschland liegt bei IT-Investitionen weit hinten, Fokus Volkswirtschaft Nr. 352, KfW Research.

[2] Vgl. Zimmermann, V. (2022): KfW-Digitalisierungsbericht Mittelstand 2021 Corona-Pandemie löst Digitalisierungsschub aus, die Digitalisierung wird aber nicht zu einem Selbstläufer, KfW Research.

[3] Vgl. Zimmermann, V. (2022): Digitalisierungsstrategien in kleinen, regional agierenden und nicht-innovativen Unternehmen selten, Fokus Volkswirtschaft Nr. 382, KfW Research.

[4] Vgl. Zimmermann, V. (2022): Erwartete Verschiebung der Nachfrage hin zu digitalen Angeboten beschleunigt die Digitalisierung im Mittelstand, Fokus Volkswirtschaft Nr. 372, KfW Research.

[5] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022.

[6] Vgl. die Studie Schwartz, M. (2016): Chancen der Digitalisierung nutzen: Datenschutz und IT-Sicherheit gehören dazu, Fokus Volkswirtschaft Nr. 117, KfW Research, die auf einer Zusatzerhebung zum KfW-Mittelstandpanel basiert.

[7] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022.

[8] Dazu zählen z. B. Mediendienstleister, IT- und Informationsdienstleister sowie Rechts-, Steuer- und Unternehmensberatungen.

[9] Dazu gehören zählen z. B. die Wirtschaftszweige Maschinenbau, Elektrotechnik oder Chemie.

[10] Vgl. Zimmermann, V. (2022), KfW-Digitalisierungsbericht Mittelstand 2021 Corona-Pandemie löst Digitalisierungsschub aus, die Digitalisierung wird aber nicht zu einem Selbstläufer, KfW Research, Zimmermann, V. (2022), Digitalisierungsstrategien in kleinen, regional agierenden und nicht-innovativen Unternehmen selten, Fokus Volkswirtschaft Nr. 382, KfW Research sowie Zimmermann, V. (2021), Künstliche Intelligenz: hohe Wachstumschancen, aber geringe Verbreitung im Mittelstand, Fokus Volkswirtschaft Nr. 318, KfW Research.

[11] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022.

[12] Ein Maß für den erreichten Digitalisierungsgrad eines Unternehmens liegt in der Erhebung nicht vor.

[13] Vgl. Zimmermann, V. (2022), Mittelständische Unternehmen mit Digitalisierungsstrategie gehen die Digitalisierung aktiver an, Fokus Volkswirtschaft Nr. 387, KfW Research.

[14] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit in Deutschland 2022.

[15] Vgl. Köhler et al. (2021): IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie.

[16] Vgl. Leifels, A. (2021): Engpässe bei Digitalkompetenzen im Mittelstand – mehr Weiterbildung nötig, Fokus Volkswirtschaft Nr. 346, KfW Research oder Zimmermann, V. (2022), Vielfältige Hemmnisse bremsen die Digitalisierung im Mittelstand, Fokus Volkswirtschaft Nr. 380, KfW Research.

[17] Vgl. Köhler et al. (2021): IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie.

[18] Vgl. Köhler et al. (2021): IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, für die detaillierte Ableitung der konkreten Handlungsempfehlungen.

[19] Vgl. Zimmermann, V. (2022), Vielfältige Hemmnisse bremsen die Digitalisierung im Mittelstand, Fokus Volkswirtschaft Nr. 380, KfW Research.