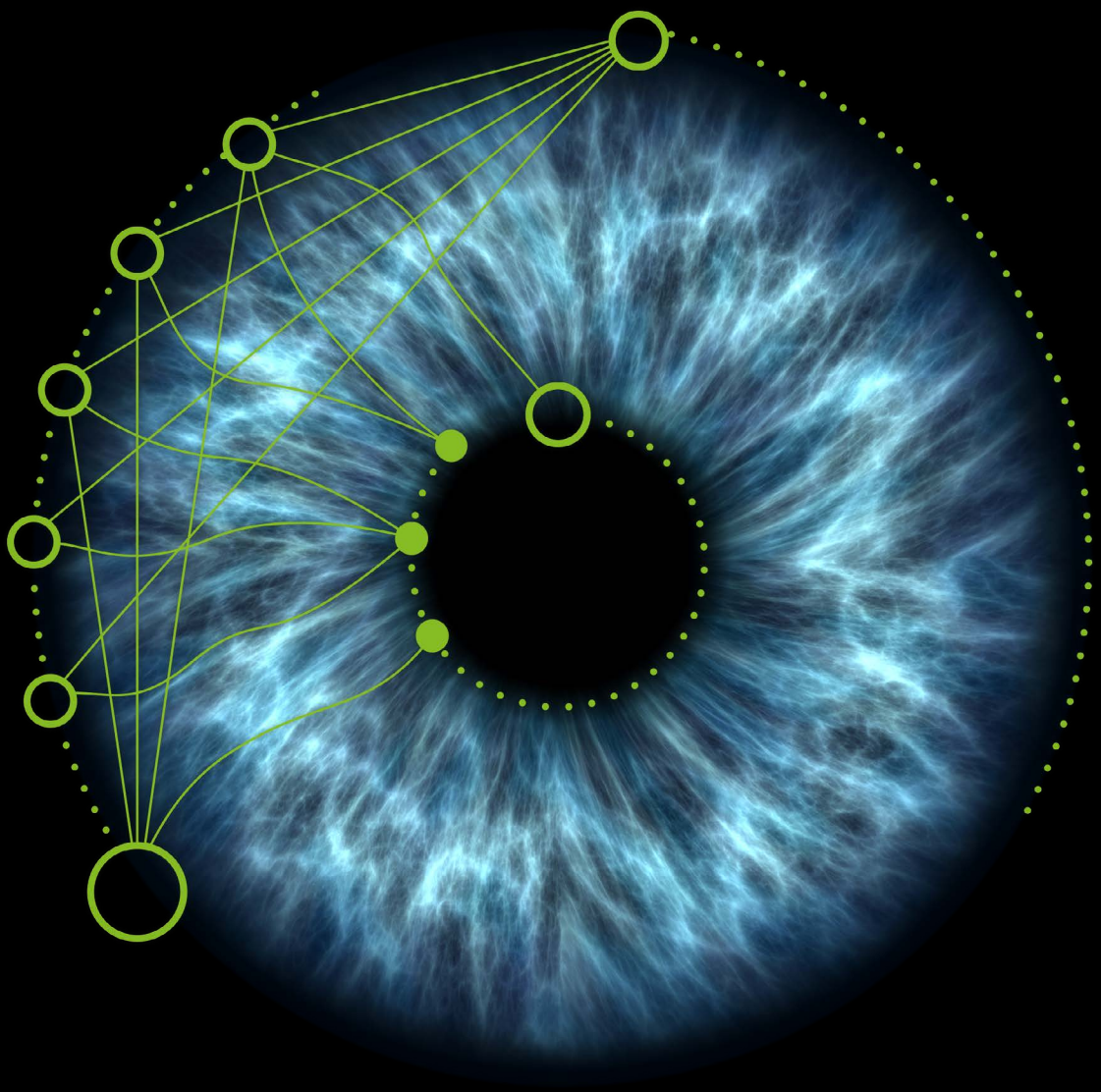
Deloitte.
Private



Cyber Security im Mittelstand

Aus der Studienserie „Erfolgsfaktoren im Mittelstand“

Forschungs-methoden

Anwendungsorientierte Mittelstands-definition und Forschungsmethoden
Für das Forschungsobjekt Mittelstand gibt es vielfältige Abgrenzungsmerkmale. So hat die Europäische Union im Jahre 2003 Unternehmen mit 50 bis 249 Beschäftigten und bis zu 50 Mio. Euro Jahresumsatz als „Mittlere Unternehmen" definiert. Eine große Anzahl typisch mittelständischer Unternehmen in Deutschland mit deutlich mehr Beschäftigten und höherem Jahresumsatz, aber vorhandener Orientierung an Eigentümer und ggf. einer Unternehmerfamilie wird damit nicht erfasst. Aus Forschungsgesichtspunkten und aufgrund ihrer Relevanz für die anwendungsorientierte Mittelstandsforschung definiert Deloitte eigentümergeführte Unternehmen und managementgeführte Unternehmen mit Eigentümereinfluss ab einer Umsatzgröße von etwa 50 Mio. Euro und einer Mitarbeiterzahl ab etwa 300 als „mittelständisch". Diese Unternehmen können sowohl eigentümergeführt als auch managergeführt sein.

Fragebögen
Um der Aktualität und Relevanz der Cyber Security im Mittelstand Rechnung zu tragen, wurde im Zeitraum Oktober–Dezember 2019 eine empirische Erhebung zu aktuellen Fragen im Kontext von Cyber-Risiken und potenziellen Abwehrmaßnahmen durchgeführt. Das Interesse der Unternehmenspraxis an dieser Fragestellung lässt sich am Rücklauf von 353 verwertbaren Online-Fragebögen erkennen, wobei nicht alle Befragten den Fragebogen komplett ausgefüllt haben. Der Mittelwert der Mitarbeiterzahl der Studienteilnehmer lag bei 1.559, der des Umsatzes bei 387 Mio. Euro. 82 Prozent der Befragten waren Mitglieder der ersten oder zweiten Führungsebene – mehrheitlich aus dem IT- (54%) sowie dem kaufmännischen Bereich (28%).

Experteninterviews
Die Erkenntnisse der Fragebogenaktion wurden in vertiefenden Experteninterviews analysiert. Hier konnten insgesamt sechs Experten gewonnen werden. Die Ergebnisse werden über konkrete Anwendungsbeispiele und persönliche Zitate in die Studie eingebunden. Folgende Experten wurden im Rahmen der Studie befragt:

- Erich Burth, Geschäftsführender Gesellschafter, RVM Versicherungsmakler GmbH & Co.
- Prof. Dr. Roland Hellmann, Professor für Informatik/Schwerpunkt IT-Sicherheit, Hochschule Aalen
- Moritz Huber, Leiter der Zentralen Ansprechstelle Cybercrime (ZAC), Landeskriminalamt Baden-Württemberg
- Alexander Iskender, IT-Verantwortlicher in einer Konzernfunktion und Cyber-Experte
- Ralph Noll, Partner im Bereich Cyber Risk, Deloitte
- Norbert Weichele, Geschäftsführer Operations & Finance, Zentis GmbH & Co. KG

Vorwort

Mittelständische Unternehmen sind die wahren Erfolgsträger der deutschen Wirtschaft.

Sie unterscheiden sich von Großunternehmen nicht nur durch ihre Betriebsgröße, sondern auch durch qualitative Besonderheiten wie spezifische Führungskultur, große Flexibilität und hohe Innovationskraft. Der deutsche Mittelstand hat eine eigenständige Problemlandkarte und besondere Erfolgsfaktoren, die empirisch zu überprüfen und in ihrer Entwicklung zu beobachten sind. Dieser Fragestellung nimmt sich Deloitte mit der Studienreihe „Erfolgsfaktoren im Mittelstand" an. Der aktuell 16. Band der Reihe (frühere Studien finden Sie unter www.deloitte.com/de/mittelstand) beschäftigt sich mit dem Thema „Cyber Security im Mittelstand".

Beinahe täglich erreichen uns aktuelle Meldungen zu Cyber-Angriffen auf Unternehmen, Behörden und andere Organisationen. Lange Zeit wurden Sicherheitsaspekte im Kontext des Internets und der Digitalisierung zu sehr vernachlässigt. Natürlich ist die digitale Transformation nicht aufzuhalten und generiert für die Mehrheit der Unternehmen neue Chancen sowie Ertragspotenziale. Gleichzeitig mit den erweiterten Optionen holen sich Unternehmen jedoch auch Risiken ins Haus, gegen die sie sich systemseitig, prozessual, instrumentell und auch menschlich absichern sollten.

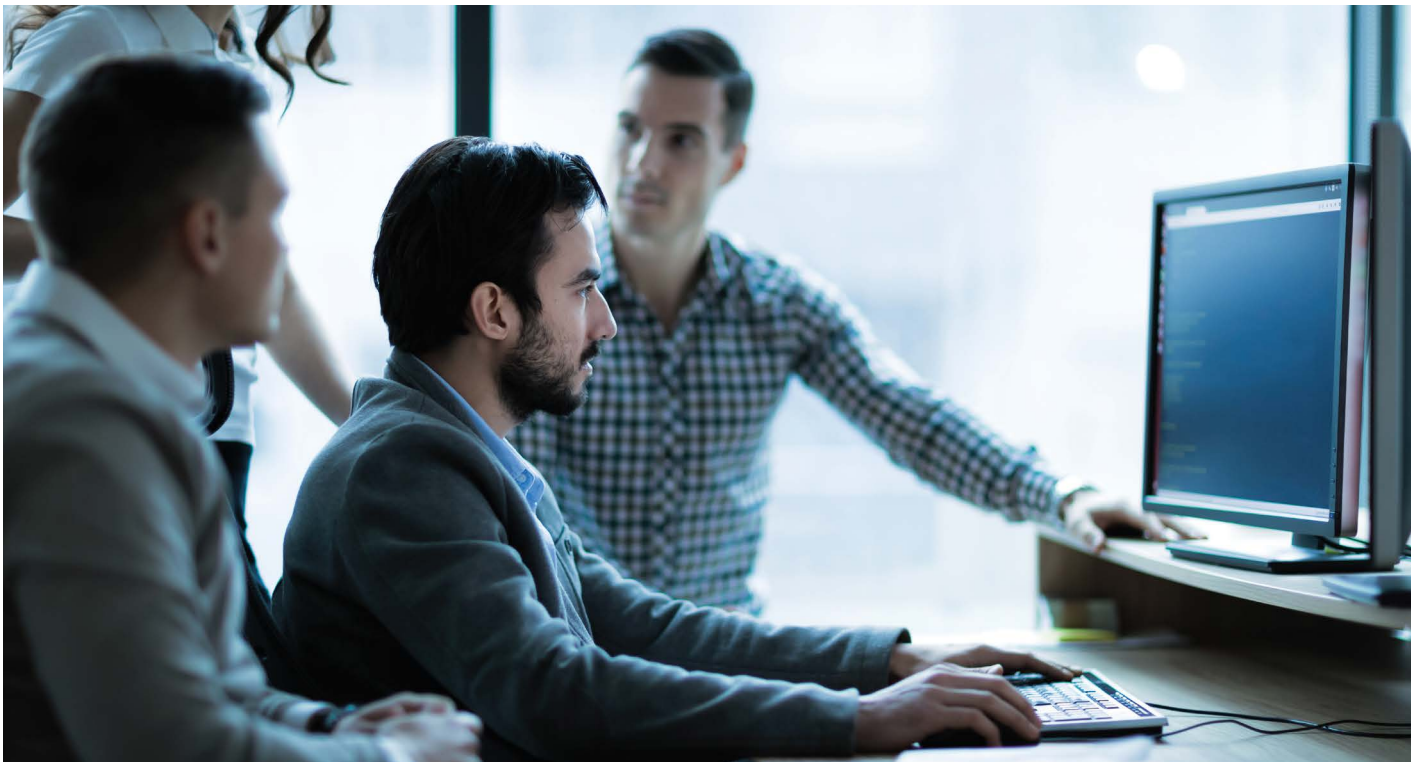
Der Mittelstand stand bisher nicht so sehr wie Großunternehmen im Blickpunkt der Öffentlichkeit, wenn es um Cyber-Attacken und Cyber Security geht. Daraus sollte man jedoch nicht folgern, dass sich Mittelständler zurücklehnen und allzu sicher fühlen dürfen. Veraltete Systeme, unzureichende Sicherheitsstandards und nicht zuletzt menschliche Fehler können auch im Mittelstand schnell zu enormen, teilweise existenzbedrohenden Situationen während eines Cyber-Angriffs oder in der unmittelbaren Folgezeit führen.

Wir gehen in der aktuell vorliegenden Studie auf der Grundlage von 353 befragten mittelständischen Unternehmen sowie sechs Fallbeispielen der Frage nach, wie mittelständische Gesellschafter und Manager die Herausforderungen, Chancen und Risiken von Cyber Security beurteilen.

Neben der besonderen Konstellation von technischen und menschlichen Risiken spielen auch Aspekte wie die faktische Bedrohungslage, der Vorbereitungsgrad verschiedener Funktionsbereiche, Budgets und nötige Investments für Cyber Security sowie etwaige Versicherungslösungen gegen Cyber-Attacken eine wichtige Rolle für unsere Überlegungen.

Ich wünsche Ihnen eine interessante und anregende Lektüre unserer Studie, die durch COVID-19 an Brisanz gewonnen hat.

Lutz Meyer
Partner
Leiter Deloitte Private



Executive Summary

Angriffe auf IT-Infrastrukturen werden nicht nur komplexer, sie nehmen in Quantität und Intensität in den letzten Jahren deutlich zu. Zur gleichen Zeit ist zu beobachten, dass immer mehr Bereiche des Alltags mit dem Internet vernetzt sind. Kaum ein Privathaushalt, kaum eine Behörde und kaum ein Unternehmen kann sich diesem Trend entziehen. Beinahe unbeachtet von der Öffentlichkeit hat somit in der jüngeren Vergangenheit das Bedrohungspotenzial durch Cyber-Attacken stetig zugenommen und nicht zuletzt mit mehreren großen Angriffen wie z.B. auf die Universität Gießen Ende 2019 oder das Kammergericht Berlin 2020 aktuell in Deutschland ein neues Rekordniveau erreicht.

Die „Opfer" derartiger Attacken sind häufig Großunternehmen, da sie in der öffentlichen Diskussion einen größeren Stellenwert einnehmen, finanziell lukrativere Ziele darstellen oder sich – ein nicht zu unterschätzender Aspekt – durch Negativschlagzeilen den Unmut potenzieller Angreifer zuziehen und somit erst zum Ziel einer Attacke werden. Da in der Presse nur sehr wenige Cyber-Attacken auf Mittelständler publik wurden, hat sich der Mittelstand an dieser Stelle bisher gesamthaft gesehen recht sicher gefühlt. Besonders seit dem Jahr 2019 haben aber Cyber-Attacken auf mittelständische und Familienunternehmen stark zugenommen.

Im Bereich Cyber Security sind Organisationen technischen, aber auch menschlichen Risiken ausgesetzt. Erstere entstehen u.a. durch veraltete Systeme, offene Schnittstellen zum Internet, unsichere Server sowie fehlende Richtlinien zum Umgang mit vertraulichen Informationen sowie physischen

Datenträgern. In der Literatur weniger stark diskutiert, dafür in der Praxis aber meist für den Erfolg einer konkreten Attacke ursächlich ist jedoch das individuelle Fehlverhalten einzelner Mitarbeiter. Unwissende oder zumindest unaufmerksame Mitarbeiter klicken auf Phishing-Links in Schad-E-Mails, verraten Passwörter an (vermeintliche) Vorgesetzte per Mail oder lassen Datenträger mit vertraulichen Inhalten unverschlossen und für alle zugänglich an ihrem Arbeitsplatz zurück.

Mittelständische Unternehmen sehen sich somit nicht nur organisatorischen, prozessualen und instrumentellen Themen gegenüber, sondern auch der Herausforderung, zeitgleich neue und im Bereich Cyber Security geschulte Mitarbeiter zu finden sowie das Sicherheitsbewusstsein der momentanen Belegschaft zu erhöhen. Während bestehende IT-Systeme und Rahmenwerke für IT-Sicherheit auf den ersten Blick einen gewissen Schutz gegen die technische sowie technologische Risikodimension von Cyber-Attacken geben, ist das individuelle Fehlverhalten von Mitarbeitern für die meisten mittelständischen Unternehmen weit schwerer zu vermeiden.

Gesamthaft gesehen werden im Mittelstand bezogen auf dieses Themenfeld aus Sicht unserer Studie die bestehenden Risiken noch immer unterschätzt. Die Befragung zeigt, dass für fast die Hälfte der Unternehmen Cyber Security nicht zu den Top-Prioritäten der Unternehmensleitung gehört und Cyber-Risiken für immerhin 48 Prozent kein zentrales Thema darstellen. Rund ein Drittel (34 Prozent) der Studienteilnehmer verfügt über keinen Reaktionsplan im Notfall. Gleichzeitig ist die Reaktionsgeschwindigkeit eine der größten Herausforderungen bei der Abwehr einer Cyber-Attacke. Doch tatsächlich sind die Unternehmen häufig nicht in der Lage, den Angreifer zu identifizieren.

Bezogen auf die Identifikation sowie Beurteilung und Vermeidung von Cyber-Risiken sind mittelständische Unternehmen recht langsam. 57 Prozent der Befragten sehen die mangelnde Reaktionsgeschwindigkeit des eigenen Unternehmens als großes Problem ihrer Organisation. Zeitgleich geben 49 Prozent an, keine Bewertungsmethode für Cyber-Risiken anzuwenden. Als größte Herausforderungen der Cyber-Abwehr werden das fehlende Sicherheitsbewusstsein der Mitarbeiter und die frühzeitige Erkennung relevanter Angriffe von je 61 Prozent der Teilnehmer gesehen. In 53 Prozent der Fälle benötigt das Unternehmen zur Aufdeckung eines relevanten Angriffs einen bis sieben Tage. Die Praxiserfahrung zeigt jedoch, dass die Systeme der Unternehmen in diesen Fällen meist bereits Jahre zuvor überwunden oder sogar übernommen wurden und dass die Angreifer erst Jahre später diesen Zugang ausnutzen.

57 Prozent der Unternehmen in der Stichprobe verfügen über keinen Notfall-Reaktionsplan und auch keine zusätzlichen, separat verfügbaren Mittel zur Abwehr von Cyber-Attacken. Wie einige aktuelle Beispiele zeigen, kann ein Cyber-Angriff jedoch die IT-Systeme von Organisationen gesamthaft lahmlegen und somit die Unternehmensexistenz bedrohen. 74 Prozent der Teilnehmer besitzen bisher kein eigenes Information Security Management System (ISMS).

Knapp die Hälfte der Unternehmen sind der Ansicht, dass insbesondere die Sensibilisierung in den Bereichen Cloud Security (45%), Sicherheit mobiler Endgeräte (44%) und Datenträger (42%) sowie im Bereich Informationsklassifizierung (42%) gering bis sehr gering ausfällt. Hierzu passen auch die recht geringen Ausgaben für Cyber Security: Deren Mittelwert liegt bei nur 80.000 Euro pro Jahr, dabei gaben sogar 40 Prozent der Unternehmen an, weniger als 10.000 Euro p.a. für Cyber Security auszugeben. Mehr als die Hälfte der Studienteilnehmer (51%) planen keinen Investitionsanstieg. Ebenfalls frappierend ist, dass nur 28 Prozent der Unternehmen angeben, eine Versicherung gegen Cyber-Risiken abgeschlossen zu haben.

Verbesserungspotenzial wird insbesondere bei Schulungs- und Weiterbildungsmaßnahmen gesehen. 45 Prozent der Befragten sehen diesbezüglich hohes und 41 Prozent mittlere Optimierungsmöglichkeiten. Auch bezüglich der Vermeidung von Cyber-Attacken meinen jeweils 44 Prozent der Teilnehmer, ein hohes bzw. mittleres Verbesserungspotenzial erkennen zu können. Hinsichtlich der Reaktion auf Cyber-Attacken gehen 43 Prozent von einem hohen und 42 Prozent von einem mittleren Verbesserungspotenzial aus. Die Identifikation von Cyber-Attacken betreffend sind 42 Prozent der Ansicht, auch diesbezüglich bestehe hoher Optimierungsbedarf, 44 Prozent stuft diesen als mittel ein.

Für die Zukunft wird die Relevanz von Cyber Security weiter zunehmen: Aktuell schätzen 50 Prozent der Befragten diese als hoch oder sehr hoch ein, für die Zukunft sind es 83 Prozent. Diese Bewertung schlägt sich jedoch aktuell noch nicht in der funktionalen und instrumentellen Umsetzung nieder.

Cyber Security im Mittelstand – Spannungsfelder

Die Digitalisierung verändert die Unternehmenspraxis grundlegend: Die Vernetzung der Welt nimmt zu, es entstehen neue, digitale Möglichkeiten für Produkte, Strategien und Ertragsmodelle. An dieser Stelle müssen bereits zahlreiche technische und sonstige Herausforderungen gemeistert werden. Meist weniger beachtet wird jedoch die Kehrseite der zunehmenden Digitalisierung.

Kriminelle machen sich die gestiegenen Möglichkeiten zunehmend zu eigen und haben sich von physischen Angriffen wie Diebstahl auf Straftaten im Bereich der Cyber-Kriminalität verlagert. Als Beispiel genannt seien Schadprogramme wie Emotet, das gefälschte E-Mails von Freunden, Nachbarn und Kollegen nutzt, um Unternehmenssysteme zu infizieren, Daten auszulesen und das System letztlich zu übernehmen.

In diesem Spannungsfeld aus gestiegenen Chancen und zeitgleich wachsenden Risiken bewegt sich auch der deutsche Mittelstand. Organisatorisch weisen viele Mittelständler gewachsene Strukturen auf, die sich durch eine hohe, historisch geprüfte Stabilität auszeichnen, aber technisch bisweilen nicht mehr auf dem neuesten Stand sind. Zudem besteht gerade bei kleineren Unternehmen die Gefahr, dass ihr IT-Know-how nicht immer State of the Art ist – bspw. bezogen auf notwendige Updates und aktuelle Sicherheitsrisiken. Auch sind die Möglichkeiten und Grenzen von Versicherungen gegen Cyber-Risiken nicht immer bekannt.

Ist ein Unternehmen von einer erfolgreichen Cyber-Attacke betroffen, drohen ihm nicht nur kurzfristige ökonomische Verluste sowie ein ggf. langfristiger Reputationsschaden: Einige aktuelle Beispiele, in denen die Systeme von Mittelständlern komplett lahmgelegt wurden und die Unternehmen letztlich vom Netz gehen mussten, bringen mitunter sogar unmittelbar existenzbedrohende Wirkungen mit sich. Für viele Mittelständler stellen sich nun die Fragen, ob sie auf die Herausforderungen hinreichend vorbereitet sind und welche aktuellen und zukünftigen Herausforderungen sich im technischen, organisatorischen, instrumentellen und menschlichen Bereich ergeben. Angesichts dieser interessanten Spannungsfelder stellen wir unsere Erfahrungen als Berater des Mittelstands in folgenden Bereichen auf den Prüfstand aktueller empirischer Daten:

Cyber-Risiken – technologische und menschliche Perspektive
Begriffsverständnis, Priorisierung, Risikobewusstsein und das Nebeneinander von technologischen Aspekten und menschlichem Fehlverhalten: Die Einschätzungen der Befragten zu diesen Aspekten lesen Sie in Kapitel I.

Bedrohungs- und Verlustszenarien – wie gut vorbereitet ist der Mittelstand?
Cyber-Attacken können aus mehreren verschiedenen Richtungen kommen, der Mittelstand ist jedoch sehr heterogen darauf vorbereitet. Für den Ernstfall haben Unternehmen z.T. auch Notfallpläne etabliert. Wie diese aussehen können und ob sie in einem konkreten Bedrohungsfall helfen, stellen wir in Kapitel II auf die Probe.

Budget und Cyber-Versicherungen – welche konkreten Pläne hat der Mittelstand?
Um sich gegen Cyber-Risiken abzusichern, sind für mittelständische Unternehmen häufig zusätzliche Investitionen in Systeme und Schulungen notwendig. Zudem besteht die Möglichkeit, sich mit speziellen Versicherungen gegen die Folgen von Cyber-Attacken abzusichern. Details zu diesen Entwicklungen lesen Sie in Kapitel III.

Ein Blick in die Zukunft – quo vadis Mittelstand?
Die Zukunftsperspektive von Cyber Security ist komplex und dynamisch. In Kapitel IV geben wir einen Ausblick auf die Selbsteinschätzung der Zukunftsperspektive durch den Mittelstand.

I. Cyber-Risiken – technologische und menschliche Perspektive

In den letzten Jahren hat die öffentliche Aufmerksamkeit für Cyber Security zwar zugenommen, das Thema hat jedoch im größeren Feld der Digitalisierung bislang nur eine Rolle am Rand der Diskussion gespielt. Seit einiger Zeit hat sich das geändert und auch die Bundesregierung hat mit dem IT-Sicherheitsgesetz 2.0 einen deutlichen Vorstoß in Richtung größerer IT-Sicherheit gemacht. Für den Mittelstand sind zunächst Konstrukte wie IT-Sicherheit, Cyber Security und Cyber-Risiken schwer greifbar und zudem recht ähnlich. Wenn schon die Begrifflichkeiten vage sind, gilt dies umso mehr für die Umsetzung der Konzepte in der Praxis. Wie gut ist der Mittelstand für die zunehmende Gefahr durch Cyber-Attacken sensibilisiert? Um diese Fragen zu beantworten, müssen zunächst Begriff und Konzept der Cyber Security näher erläutert und auf ihre Relevanz für den Mittelstand hin untersucht werden. Aus diesem Grund widmen wir uns in diesem Kapitel neben der Einschätzung und Definition des Begriffs auch der Einordnung von Trends und Veränderungen im Umfeld mittelständischer Unternehmen und der Einschätzung der aktuellen Priorität für Unternehmen. Das Spannungsfeld Technologie vs. Mensch soll hier besonders im Fokus der Überlegungen stehen.

Begriffsverständnis und Priorität von Cyber Security

Begriff und Konzept der Cyber Security sind auf den ersten Blick weit weniger klar als bei verwandten Konstrukten wie z.B. der IT-Sicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt fest, dass sich Cyber Security (synonym: Cyber-Sicherheit) mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik befasst. Das Aktionsfeld der klassischen IT-Sicherheit wird hierbei auf den gesamten Cyber-Raum ausgeweitet und umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik. Es schließt somit darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

In der englischen Sprache hingegen hat der deutsche Begriff der IT-Sicherheit zwei verschiedene Ausprägungen.

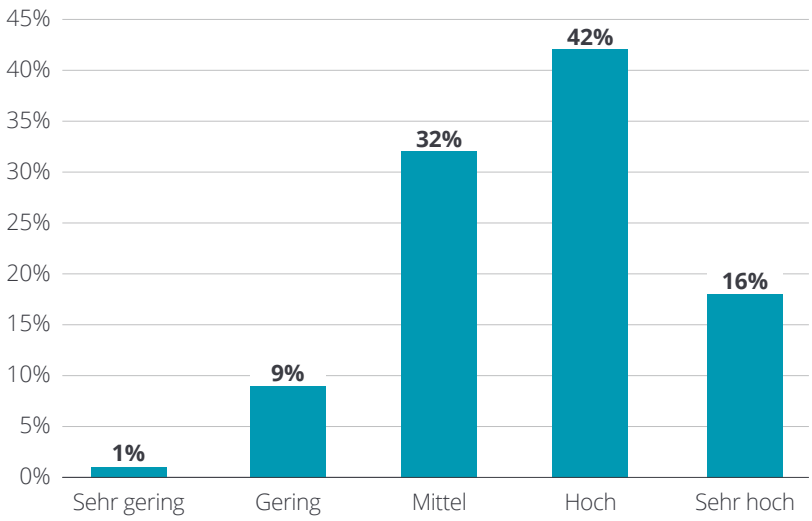
- **Funktionssicherheit** (Safety) stellt sicher, dass sich ein spezifisches System konform zur erwarteten Funktionalität verhält.
- **Informationssicherheit** (Security) bezieht sich auf den Schutz der technischen Verarbeitung von Informationen und ist eine Eigenschaft eines funktionssicheren Systems.

„Oft wird dem Unterschied zwischen Security und Safety nicht genügend Wert beigemessen. Bei Fahrzeugen ist die Safety im Sinne von funktionaler Sicherheit seit Langem allgegenwärtig: Insassen dürfen nicht gefährdet werden. Im Zweifelsfalle wird das Fahrzeug in einen als sicher definierten Zustand versetzt, z.B. angehalten. Dazu nötige Funktionalitäten werden vorgegeben, umgesetzt und getestet. Was oft nicht ins Blickfeld gerät, ist die Abwesenheit unerwünschter Funktionalitäten. Genau das ist aber, was Security ausmacht: Es darf keine Hintertüren, Seiteneffekte und Ähnliches geben. Um das zu gewährleisten, benötigt man eine andere Herangehensweise bereits ab dem Beginn des Entwicklungsprozesses."

Prof. Dr. Roland Hellmann
Hochschule Aalen

In unserer Studie haben wir die aktuelle Priorität von Cyber Security für die mittelständische Praxis hinterfragt. Wie Abbildung 1 zeigt, schätzen die Teilnehmer die Priorität im Unternehmen mehrheitlich hoch (42%) oder mittel (32%) ein. Interessant erscheint zudem, dass doch 10 Prozent die Priorität der Cyber Security als niedrig oder sehr niedrig bewerten. Hier kann ggf. ein mangelndes Problembewusstsein für die Thematik vorliegen.

Abb. 1 – Priorität von Cyber Security für die Unternehmen



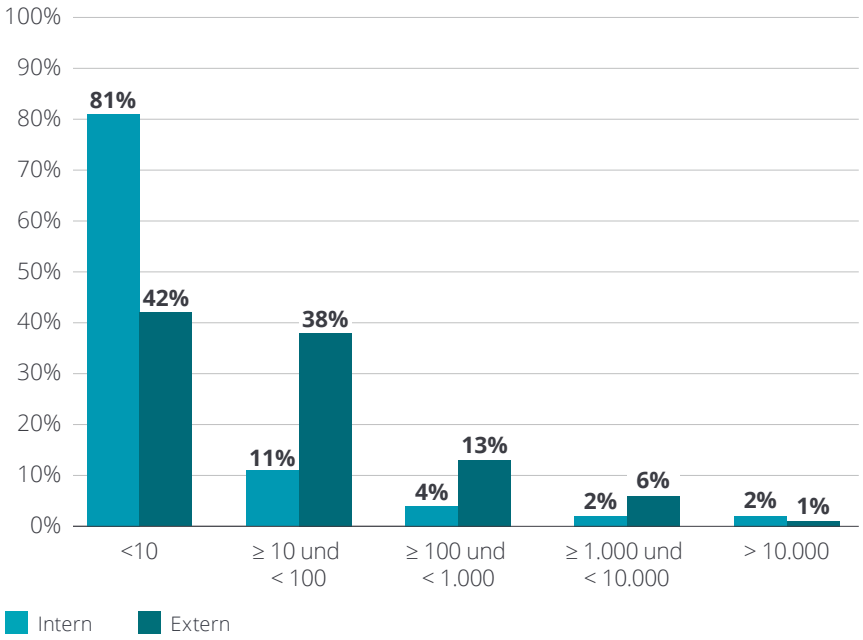
Art und Umfang von Cyber-Attacken

Prinzipiell ist es für Unternehmen sehr schwierig, Cyber-Attacken überhaupt zu entdecken. In vielen Fällen befinden sich Angreifer bereits sehr lange im System, bevor sie den eigentlichen „Angriff" starten. Dieser kommt dann häufig plötzlich und trifft die Unternehmen meist unvorbereitet. Wie unsere Studie zeigt (vgl. Abb. 2), ist zumindest in der Stichprobe die Anzahl der internen und externen Attacken verhältnismäßig klein. Mit Attacken sind hier keine Fehler gemeint, sondern gezielte, bösartige Angriffe von internen oder externen Personen. In 81 Prozent der Unternehmen finden weniger als zehn interne und in 42 Prozent weniger als zehn externe Attacken pro Unternehmen statt. Diese werden dann meist durch Virenscanner oder speziell geschulte Teams identifiziert. Teilweise werden auch Gegenmaßnahmen wie die gezielte Attacke auf einen Angreifer unternommen.

„Für eine erfolgreiche Umsetzung von Cyber Security muss zunächst eine Awareness bei allen Beteiligten für das Thema geschaffen werden."

Norbert Weichele
Zentis GmbH & Co. KG

Abb. 2 – Anzahl der Attacken in Unternehmen



„Für die meisten Unternehmen ist es beinahe unmöglich, die konkrete Identität von Cyber-Angreifern zu ermitteln."

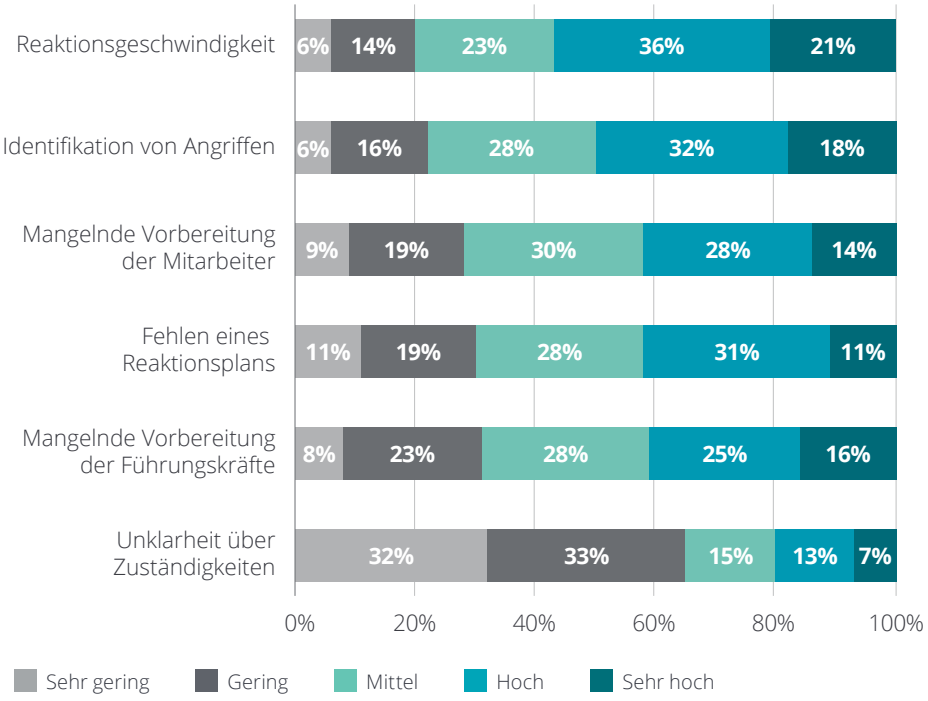
Ralph Noll
Deloitte

Insgesamt gesehen gehört die Identifikation von Attacken zu den größten Herausforderungen, denen Unternehmen in diesem Kontext gegenüberstehen. Wie unsere Studie zeigt (vgl. Abb. 3), sehen 57 Prozent der Befragungsteilnehmer die Reaktionsgeschwindigkeit, die Identifikation von Attacken (50%), die mangelnde Vorbereitung der Mitarbeiter (42%) sowie das Fehlen eines Reaktionsplans (42%) als größte Herausforderungen (jeweils als „hoch" oder „sehr hoch" bewertet). Die Sensibilisierung der Führungskräfte sowie die Klärung von Zuständigkeiten in Unternehmen scheinen hingegen weniger problematisch zu sein.

„Sicherheitslücken entstehen oft durch Schwächen bei der Softwareentwicklung. Programmierer sind meistens keine IT-Sicherheits-Experten."

Prof. Dr. Roland Hellmann
Hochschule Aalen

Abb. 3 – Herausforderungen bei Cyber-Attacken



Relativ häufig wurde in unserer Befragung das Spannungsfeld von technischen und menschlichen Herausforderungen thematisiert. Die Studienteilnehmer als auch die interviewten Experten berichten, dass beide Aspekte gleich wichtig sind, dass aber gerade die Mitarbeiter in mittelständischen Unternehmen eine doppelte Gefahr darstellen: Einerseits sind sie nicht immer für die von Cyber-Attacken ausgehenden Gefahren sensibilisiert oder unterschätzen diese stark. Andererseits sind Aktionen von Mitarbeitern in der Vielzahl der Fälle für die erfolgreiche Übernahme von Unternehmenssystemen durch Angreifer ursächlich. Dies gilt insbesondere für die aktuellen Themen Trojaner/Krypto-Logger sowie Hacks in das Unternehmensnetzwerk zur Ausspähung von Unternehmensgeheimnissen. Selbst die IT-Mitarbeiter von Unternehmen sind davon nicht ausgenommen.

Zusätzlich thematisiert wurde in der Studie die Priorität von Cyber-Risiken für die Unternehmenssteuerung (vgl. Abb. 4). Diese wird von 53 Prozent der Unternehmen als hoch oder sehr hoch und von 36 Prozent zumindest als mittelhoch eingeschätzt. Dabei sind sich die Befragten einig, dass das Thema Chefsache ist und auf die Agenda von Vorstand, Geschäftsführung und Aufsichtsrat gehört.

Die Frage nach der Priorität von Cyber-Risiken haben wir in der Folge auch genutzt, um zwei Gruppen von Unternehmen zu bilden: solche, bei denen diese Risiken eine hohe oder sehr hohe Priorität besitzen, und die, bei denen die Einschätzung von mittel bis sehr gering variiert. Wir werden einzelne Studienergebnisse gezielt nach diesem Kriterium interpretieren.

Zum erfolgreichen Umgang mit Cyber-Risiken gehört auch die finanzielle Bewertung der mit den Attacken verbundenen Gefahren. Hier zeigt sich (vgl. Abb. 5), dass 49 Prozent der Unternehmen keine Bewertungsmethodik für Cyber-Risiken einsetzen. Immerhin 16 Prozent beschreiben die möglichen Gefährdungen. Eine ökonomische Quantifizierung gelingt bisher nur 12 Prozent der Studienteilnehmer. Hier besteht sicherlich noch Verbesserungspotenzial.

Abb. 4 – Priorität von Cyber-Risiken

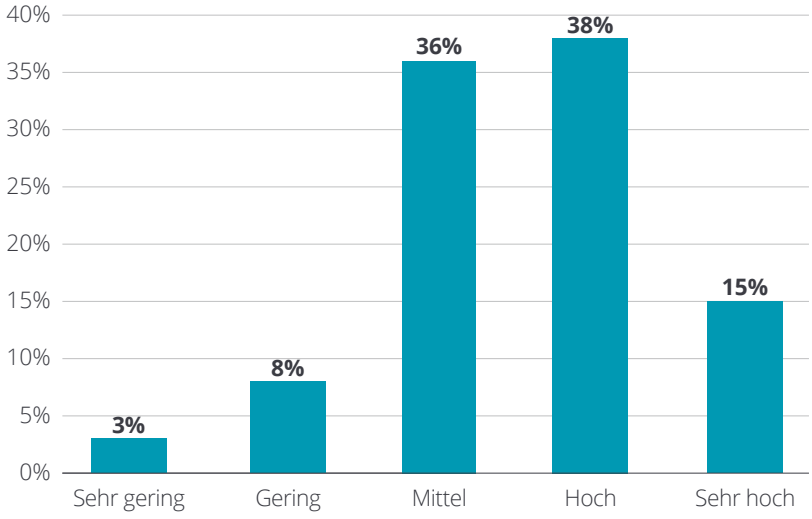
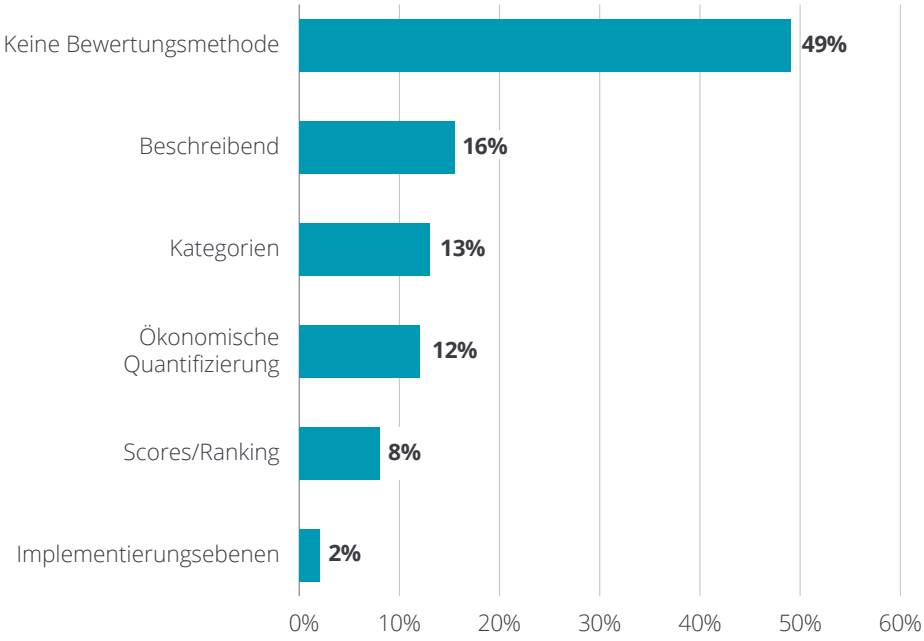


Abb. 5 – Bewertung von Cyber-Risiken

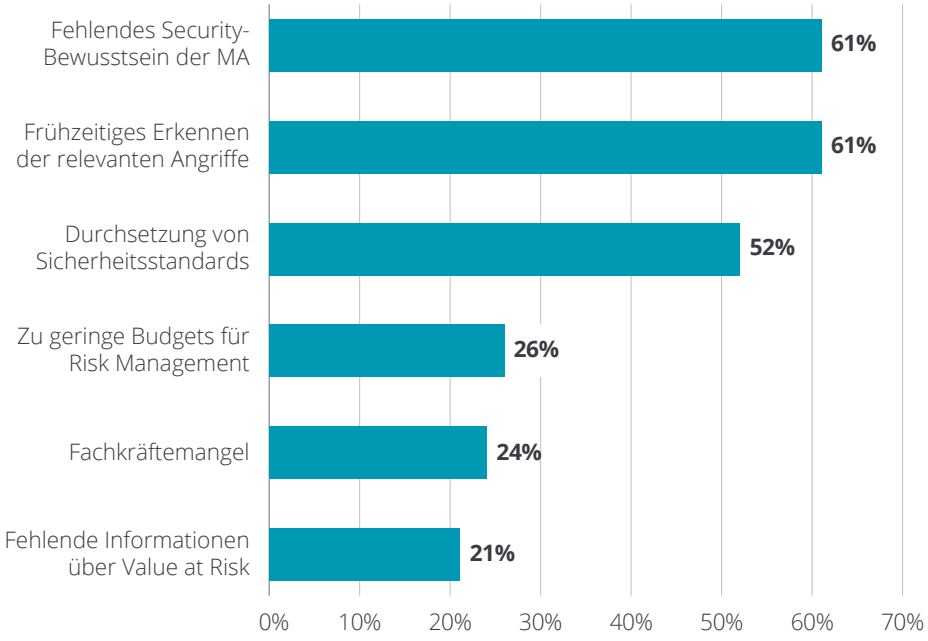


Abwehr von Cyber-Risiken

Erst nach dem Erkennen und der Bewertung von Cyber-Attacken – die im Mittelstand wie bereits aufgezeigt an sich bereits problematisch sind – kann das Unternehmen versuchen, diese wirksam abzuwehren. Hierbei wären natürlich die Prävention und somit die Verhinderung von Attacken einem Management bereits erfolgter und erfolgreicher Attacken vorzuziehen. Hier zeigt sich, dass die reine Technik an sich nicht ausreicht, um die „Schwachstelle Mensch" zu kompensieren.

In der Studie (vgl. Abb. 6) nennen die Unternehmen das fehlende Sicherheitsbewusstsein der Mitarbeiter als auch die frühzeitige Erkennung von Angriffen mit je 61 Prozent als größte Herausforderungen im Rahmen der Abwehr. Die Umsetzung von Sicherheitsstandards wie ISO 27001 oder COBIT (Framework für IT-Governance und -Compliance) sehen 52 Prozent der Befragten als Problem. Die geringen Budgets, der Fachkräftemangel sowie fehlende Informationen zur Quantifizierung des ökonomischen Schadenspotenzials werden je von etwa einem Viertel bzw. Fünftel der Befragten genannt.

Abb. 6 – Größte Herausforderungen bei der Abwehr von Cyber-Risiken

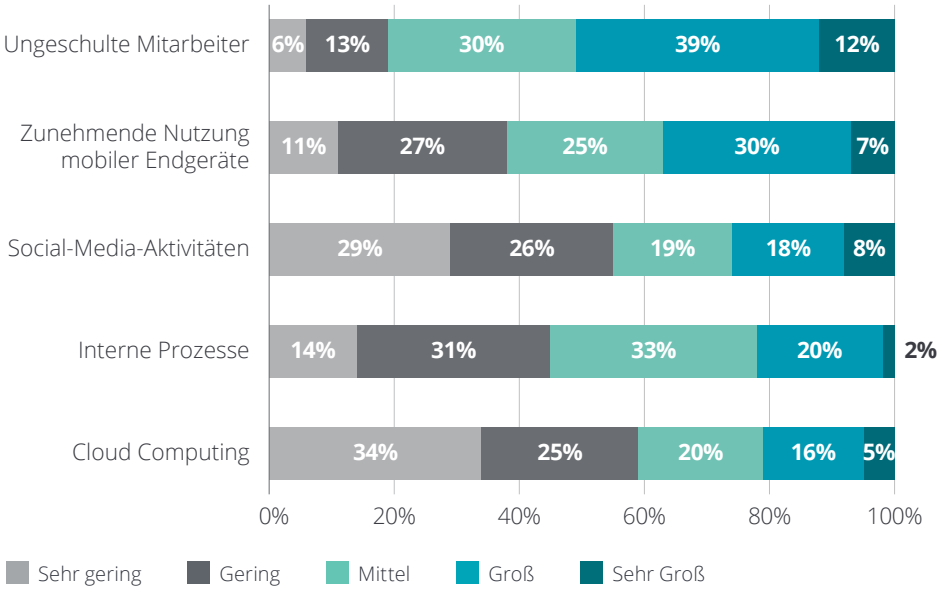


„Aufgrund ihres spezifischen Know-hows stellen KMUs für Cyber-Angreifer häufig lukrative Ziele dar."

Moritz Huber
LKA Baden-Württemberg

Wie bereits im Deloitte Cyber Security Report 2019 festgestellt wurde, besteht in Unternehmen parallel eine Vielzahl von Sicherheitslücken. In dieser Studie (vgl. Abb. 7) ist erneut ein Nebeneinander von menschlichen und technischen Gefahrenherden zu erkennen. 51 Prozent der Unternehmen geben ungeschulte Mitarbeiter als größte Sicherheitslücke an. Hinzu kommen mit 37 Prozent die Nutzung mobiler Endgeräte sowie mit 26 Prozent die Social-Media-Aktivitäten von Mitarbeitern. Diese im Vergleich zu anderen Studien und unserer Praxiserfahrung relativ geringen Zahlen lassen uns zu dem Schluss kommen, dass hier die Gefahrenlage deutlich unterschätzt wird.

Abb. 7 – Subjektive Sicherheitslücken aus Sicht der Befragten

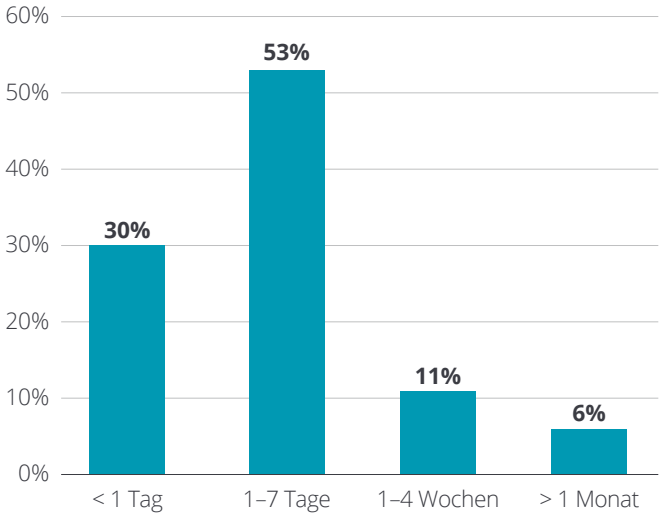


Nicht nur die Existenz von Sicherheitslücken, sondern auch deren Entdeckung spielt für eine erfolgreiche Cyber-Abwehr eine wichtige Rolle. Nach verschiedenen Studien sind Cyber-Angreifer im Schnitt bereits rund 200 Tage im System, bevor sie entdeckt werden oder es zu einem erfolgreichen Angriff kommt. In unserer Studie (vgl. Abb. 8) geben die Teilnehmer an, in 53 Prozent der Fälle Sicherheitslücken nach einem bis sieben Tagen zu entdecken. Dies klingt nach einer sehr schnellen Identifikationsrate, die deutlich im Kontrast zu anderen Studien steht. Selbst wenige Minuten oder Stunden können Angreifern schon ausreichen, um Daten auszulesen, Schadsoftware zu installieren oder die Systeme des Unternehmens zu übernehmen.

Zu unseren Ergebnissen gehört (ohne eigene Abb.), dass Unternehmen, in denen Cyber-Risiken eine hohe Priorität genießen, signifikant schneller reagieren können: Diese sind besser vorbereitet und Sicherheitslücken werden häufig innerhalb weniger Minuten oder Stunden aufgedeckt sowie Gegenmaßnahmen eingeleitet. Ebenfalls ausgewertet wurde, wie die Sicherheitslücken entdeckt werden (ohne eigene Abb.). In 76 Prozent der Fälle gelingt dies durch automatisierte Routinen und/oder automatisiertes Verwundbarkeits- und Patch-Management. Es folgen konkrete Aktionen eines verantwortlichen Teams oder einer Einzelperson mit 68 Prozent der Nennungen. Für uns eine überraschende Rückmeldung: Immerhin 8 Prozent der Unternehmen erfahren von einem Angriff auf ihr Unternehmen aus der Presse.

Im ersten Kapitel haben wir festgestellt, dass die Awareness für Cyber-Risiken im Mittelstand recht heterogen ist. Nicht allen Unternehmen ist die Bedrohungslage bewusst. Zudem wurde klar, dass auch die besten technischen Standards nicht helfen, wenn die Mitarbeiter im Bereich Cyber-Sicherheit nicht geschult sind. Zur Vertiefung der Analyse folgt nun ein Interview mit dem Cyber-Experten Ralph Noll von Deloitte.

Abb. 8 – Entdeckung von Sicherheitslücken



„Im Rahmen unserer Ermittlungsmaßnahmen stellen wir immer wieder fest, dass die Vorbereitungsmaßnahmen der angegriffenen Unternehmen hinsichtlich Intensität und Umfang sehr unterschiedlich ausfallen. Fest steht jedoch, dass ohne präventive und reaktive Vorbereitungsmaßnahmen Cyber-Angriffe nur sehr schwer zu bewältigen sind."

Moritz Huber
LKA Baden-Württemberg

Interview mit dem Cyber-Experten Ralph Noll, Deloitte

Zur Verifikation der in der Studie thematisierten Bereiche haben wir ein Interview mit Ralph Noll geführt. Er ist Partner im Bereich Cyber Risk bei Deloitte und verantwortlicher Ansprechpartner für alle Fragestellungen rund um die Themenbereiche Cyber Resilience, Incident Response, Cyber Forensics, Cyber Investigations sowie Business Continuity Management und Red Teaming. Er hat mehr als 20 Jahre Erfahrung bei der Abwehr von Cyber-Angriffen und der Durchführung digitaler forensischer Untersuchungen sowie bei der Vorbereitung von Organisationen auf solche Krisensituationen, insbesondere im internationalen Kontext.

Ist der Mittelstand durch Cyber-Attacken besonders stark bedroht?
Grundsätzlich sind über alle Industrien hinweg alle Unternehmensgrößen betroffen, allerdings gilt für bestimmte Branchen wie bspw. Telekommunikationsunternehmen, Kreditinstitute und Versicherungen sowie die Gesundheitsbranche eine besonders starke Bedrohungslage durch Cyber-Attacken. Der Unterschied ist, dass Großunternehmen deutlich mehr Ressourcen und Know-how zu deren Erkennung und Abwehr besitzen.

Inwiefern sind aus Ihrer Sicht mittelständische Unternehmen auf Cyber-Attacken vorbereitet (technisch, organisatorisch, menschlich, prozessual, finanziell, versicherungstechnisch)?
Nach unserer Wahrnehmung haben die mittelständischen Unternehmen seltener Sicherheitskonzepte oder Notfallpläne, um strukturiert auf einen Cyber-Angriff zu reagieren. Das variiert allerdings sehr stark nach Branche und unterschiedlichem Reifegrad des Unternehmens.

Von welchen Quellen (Stichworte Hacker, Insider) gehen für mittelständische Unternehmen die größten Sicherheitsrisiken aus?
Die Quellen für Sicherheitsrisiken sind stark unternehmensabhängig. Es kann aber gesagt werden, dass Hacker stets das schwächste Glied angreifen. Dafür analysieren sie das ausgewählte Unternehmen sogar Monate im Voraus und befinden sich im Durchschnitt 192 Tage im System, bevor sie agieren. Eine genauere Feststellung des Ausgangspunkts eines Cyber-Angriffs ist in den meisten Fällen aber nur schwer bis kaum möglich.

Wird die menschliche Komponente (Mitarbeiterverhalten) im Bereich Cyber Security unterschätzt?
Ja, die meisten definierten Prozesse, die Unternehmen zur Identifikation und Bewertung von Cyber-Risiken einsetzen, dienen nur der Netzwerküberwachung und Schwachstellenanalyse der Geschäftsanwendungen. Viele Angriffe sind nur erfolgreich, weil menschliche Fehleinschätzung, mangelndes Risikobewusstsein, Bequemlichkeit oder bewusster Missbrauch dies ermöglichen. Awareness-Trainings oder Simulationen im Hinblick auf potenzielle Risiken können viel verhindern, finden aber kaum statt.

Welche konkreten Risiken (z.B. mobile Endgeräte, Social Media, Phishing) halten Sie im Mittelstand für besonders relevant?
Wir konnten in unserem Cyber Security Report von 2019 ermitteln, dass die Manipulation durch Fake News und der Datenbetrug im Internet die größten Risiken für mittelständische Unternehmen darstellen. Auch sind die Bereiche Cloud und Social Engineering besonders relevant, da diese oftmals unterschätzt werden. Besondere Probleme im Mittelstand sind auch CEO/CFO Fraud und Ransomware-Attacken, die das gesamte Unternehmen lahmlegen.

Wie sieht aus Ihrer Sicht ein effektiver und effizienter Maßnahmen- und Notfallplan im Fall einer Cyber-Attacke aus?
Ein effizienter Notfallplan sollte Handlungsschritte für die Wiederherstellung der Geschäftsprozesse sowie die Priorität, mit der diese Schritte erfolgen müssen, und die zugehörige Verantwortlichkeit beinhalten. Genauere Handlungsschritte könnten bspw. Schritte zur Inbetriebnahme eines Ausweichrechenzentrums oder die Etablierung eines Cyber-Incident-Response-Teams sein. Rahmenbedingungen und Entscheidungshilfen kann das Krisenmanagement einem extra dafür angefertigten Krisenstabsleitfaden entnehmen, außerdem kann dieser Kontaktdaten der zuständigen Behörden beinhalten. Für den Notfall sollte auch ein Krisenkommunikationsplan zur Berichterstattung an die Außenwelt bestehen.

Wer sollte Cyber Security verantworten und warum?
Durch die voranschreitende Digitalisierung sind Cyber-Risiken schon längst zu Business-Risiken geworden, weshalb Cyber Security in der Geschäftsleitung, in Form eines CISO, verankert werden sollte. Des Weiteren sollte die regelmäßige Bewertung der Cyber-Sicherheitslage in Aufsichtsräten etabliert werden.

Kann und sollte man sich gegen Cyber-Attacken versichern? Wie teuer ist das? Was sind die Voraussetzungen?
Eine Versicherung kann eine von vielen Maßnahmen zum Management der Risiken im Cyber-Umfeld sein. Allerdings deckt eine solche einige Risiken wie bspw. die Reputationsschäden nicht ab. Die Kosten sind stark von der Bedrohungslage und dem Reifegrad des Unternehmens zur Erkennung und Abwehr von Bedrohungen abhängig.

Wo sehen Sie im Bereich Cyber Security im Mittelstand die größten Handlungsbedarfe?
Der größte Handlungsbedarf liegt im Bereich der Erkennung von Attacken, da auftretende Anomalien erkannt und analysiert werden müssen, bevor es zu einer Reaktion auf Cyber-Angriffe kommen kann. Die dann notwendige Routine für die angemessene Reaktion kann durch regelmäßige Simulationen wie War Gaming oder Red Teaming erlangt werden. Außerdem sollten Awareness-Trainings im Hinblick auf die größten Risiken für das jeweilige Unternehmen stattfinden.

Wie viel sollte man für Cyber Security pro Jahr ausgeben, damit man gut geschützt ist?
Das angemessene Budget hängt sehr von dem jeweiligen Geschäftsmodell und der damit einhergehenden Bedrohungslage ab und kann nur unternehmensspezifisch bestimmt werden. Aber ein Richtwert lässt sich schon nennen: Gemäß einer Studie geben Unternehmen im Durchschnitt 10 Prozent vom IT-Budget für Cyber Security aus, was nach unserer Meinung eher am unteren Ende unserer Empfehlung von 5 bis 20 Prozent des IT-Budgets liegt.

II. Bedrohungs- und Verlustszenarien – wie gut vorbereitet ist der Mittelstand?

Zunächst sind wir auf die prinzipielle Einschätzung des Mittelstands zur Cyber Security eingegangen. In diesem Kapitel wollen wir uns mit konkreten Bedrohungs- und Verlustszenarien auseinandersetzen und auch darauf eingehen, mit welchen Maßnahmen Mittelständler proaktiv, reaktiv und ggf. sogar präventiv mit Cyber-Attacken umgehen können. Hierzu gehört auch ein realistischer Abgleich der Selbsteinschätzung des Mittelstands und der Sicht der in der Studie befragten Experten zum Vorbereitungsgrad und zur Reaktionsfähigkeit mittelständischer Unternehmen.

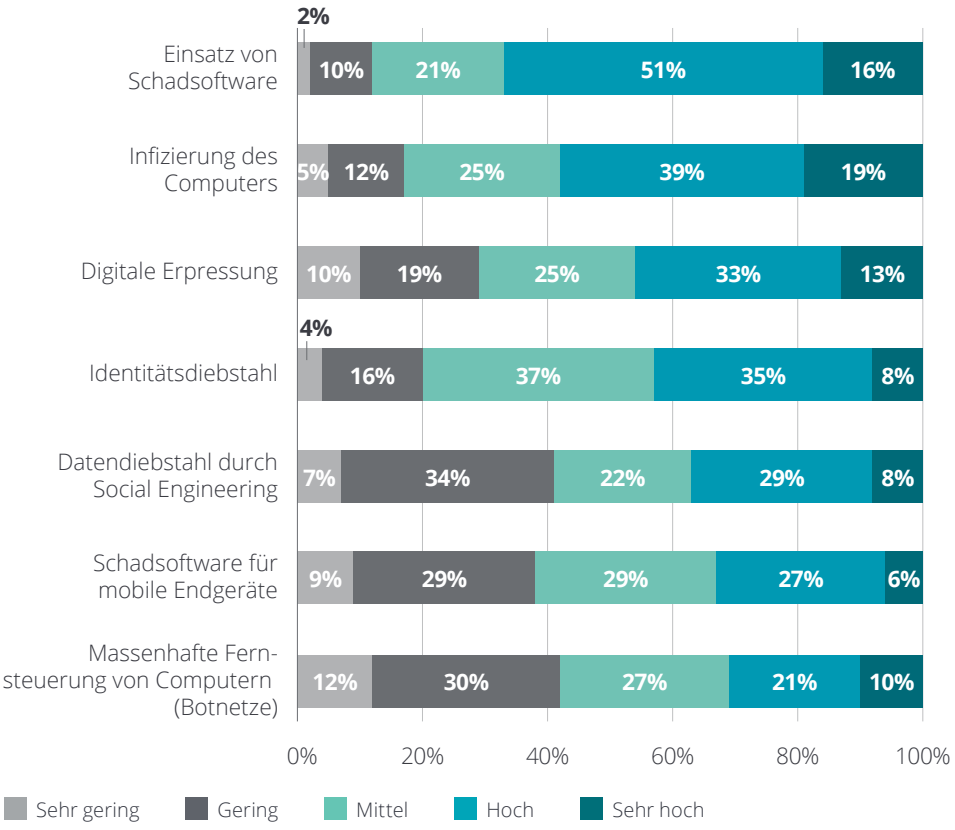
Schadenspotenzial von Cyber-Attacken

In der Tagespresse, aber auch in Fachveröffentlichungen wird aktuell eine Vielzahl verschiedener möglicher Attacken auf Unternehmen diskutiert. Für eine einzelne Organisation ist kaum überschaubar, wie sich die verschiedenen Attacken unterscheiden und welche Formen für ein Unternehmen im konkreten Fall eine Bedrohung darstellen.

In dieser Studie (vgl. Abb. 9) wird dem Einsatz von Schadsoftware mit 67 Prozent das höchste Schadenspotenzial beigemessen – Schadsoftware oder Malware bringt eine weite Bandbreite von unerwünschten oder sogar schädlichen Folgen mit sich. Es folgen mit 58 Prozent die Infizierung von Computern, die digitale Erpressung (46%), der Identitätsdiebstahl, z.B. durch Phishing ausgelöst (43%), sowie der Datendiebstahl durch Social Engineering (37%). Bei letzterer Attacke geben sich Angreifer als Vorgesetzte, Kollegen oder Freunde aus, um Daten von Mitarbeitern zu erhalten.

In unserer Studie von den Unternehmen seltener als relevant erachtet, dafür von den interviewten Experten als sehr wichtig eingestuft wurde die Fernsteuerung von Netzen durch Botnetze.

Abb. 9 – Schadenspotenzial konkreter Attacken



„Trojaner/Krypto-Logger sowie Hacks in das Unternehmensnetzwerk sind aktuell Beispiele für Attacken, die ein erhöhtes Schadenspotenzial für mittelständische Unternehmen aufweisen."

Alexander Iskender
IT-Verantwortlicher und Cyber-Experte

Reaktionsplan und strategische Perspektive

Die interviewten Experten sind sich einig, dass mittelständische Unternehmen eine Cyber-Attacke nur durch Existenz eines oder mehrerer Notfallpläne überleben können. In der Presse wurden in den letzten Monaten mehrere Fälle diskutiert, in denen Unternehmen nach dem totalen Systemausfall ad hoc umdisponieren und teilweise sogar aus dem Stand neue Unternehmensinfrastrukturen und IT-Systeme schaffen mussten, um zumindest eine teilweise Fortführung des operativen Geschäfts zu ermöglichen.

Ein Cyber-Notfallplan soll bei plötzlich eintretenden Ereignissen und Problemen im IT-Umfeld die Schäden für Organisationen, Unternehmen oder Einzelpersonen begrenzen oder – im Optimalfall – abwenden. Er stellt eine Art Handbuch mit einem Katalog von durchzuführenden Maßnahmen und Handlungsanweisungen dar. Dazu gehören u.a. technische, organisatorische, juristische, kommunikative und wirtschaftliche Maßnahmen. Diese können von der sofortigen Trennung infizierter Geräte vom Internet bis zur proaktiven Kommunikation eines Datenlecks gegenüber Kunden und anderen Stakeholdern reichen.

„Ein wirksamer Notfallplan für Cyber-Angriffe beginnt bereits lange vor dem eigentlichen Angriff selbst. Unternehmen müssen sich im Rahmen eines risikobasierten Ansatzes fragen, welche Unternehmenswerte besonders schützenswert sind und welche Angriffsszenarien sich besonders kritisch auf den Geschäftsbetrieb auswirken können. Auf dieser Basis sollten dann strategische Überlegungen durchgeführt werden, wie den identifizierten Risiken und Schadensszenarien mit den vorhandenen Ressourcen begegnet werden kann. Bei der anschließenden Umsetzung der sich hieraus ergebenden Maßnahmen stehen folgende Schwerpunkte im Fokus:

- Erstellung eines Notfallhandbuchs
- Festlegung von strategisch relevanten Kooperationspartnern (bspw. ZAC, IT-Security-Provider, IT-Dienstleister etc.)
- Festlegung von Vorkehrungen, um den Geschäftsbetrieb im Angriffsfalle (ggf. reduziert) weiterführen zu können
- Festlegung von Vorkehrungen, um nach der Bewältigung des Cyber-Angriffs den (vollumfänglichen) Geschäftsbetrieb wiederherzustellen
- Erstellung einer intern und extern ausgerichteten Krisenkommunikationsstrategie“

Moritz Huber
LKA Baden-Württemberg

In unserer Studie (vgl. Abb. 10) haben wir nach den Unternehmen mit hoher und niedriger Priorität für Cyber-Risiken kontrastiert. Während 57 Prozent der Befragten, für die Cyber Security eine hohe Bedeutung aufweist, einen Notfallplan haben, sind es in der Gruppe derer mit geringerer Priorität nur 26 Prozent. Auf alle Unternehmen bezogen weisen 43 Prozent einen Notfallplan auf (ohne eigene Abb.). Eng verbunden mit dem Vorhandensein eines Reaktionsplans ist das Vorhandensein zusätzlicher finanzieller Mittel – einer Art Notbudget – für den Fall eines erfolgreichen Cyberangriffs. Mit diesen Mitteln können Berater engagiert, kurzfristig alternative Systeme bereitgestellt und auch kommunikative Maßnahmen finanziert werden.

In der Studie (vgl. Abb. 11) sehen immerhin 70 Prozent und damit die weit überwiegende Mehrheit der Unternehmen zusätzliche Mittel für den Fall einer Cyber-Attacke vor.

Abb. 10 – Existenz eines Notfallplans (Kontrastierung nach Priorität)

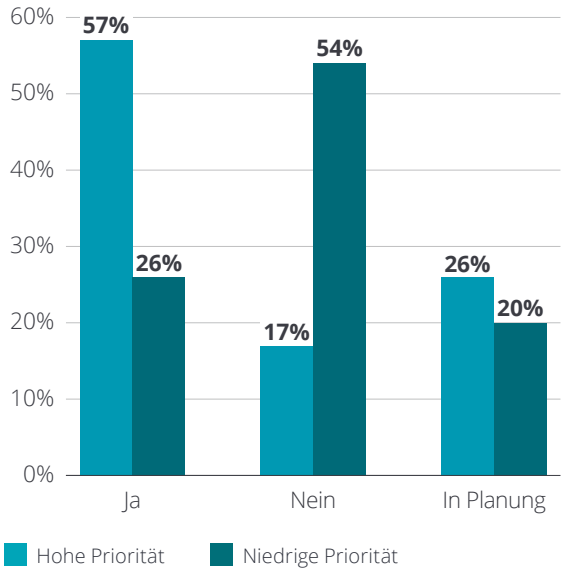
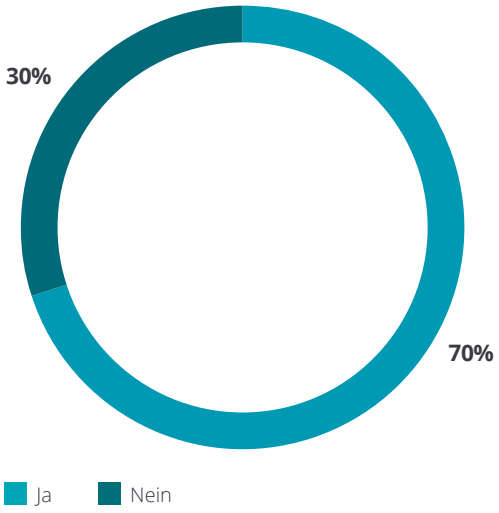


Abb. 11 – Vorhandensein finanzieller Mittel für die Abwehr einer Cyber-Attacke



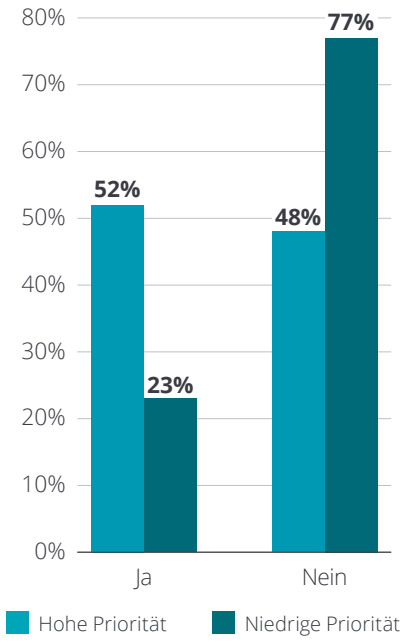
„Neben einem Informationssicherheitsmanagementsystem sollten zwingend auch IT-Notfallprozesse implementiert und geübt werden."

Moritz Huber
LKA Baden-Württemberg

Organisatorische Verantwortlichkeiten

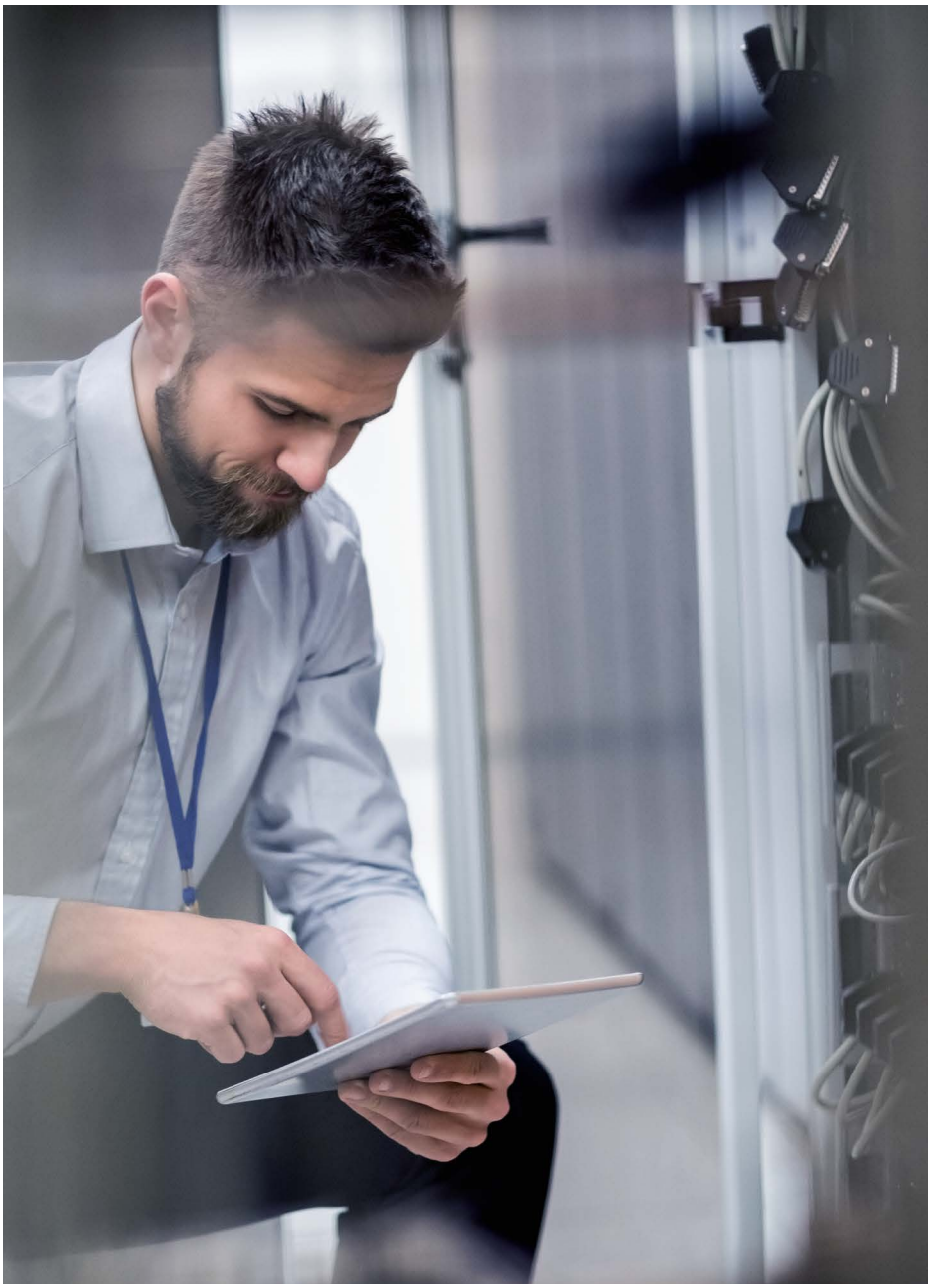
Aspekte wie Digitalisierung, Industrie 4.0, digitale Transformation und digitale Geschäftsmodelle stehen immer häufiger auf der Agenda der Top-Entscheider im Mittelstand. Dies liegt u.a. daran, dass Unternehmenssysteme gar nicht mehr vollständig vom Internet isoliert betrachtet werden können. In unserer Befragung (vgl. Abb. 12) haben wir uns auch damit befasst, ob Cyber Security Teil der Unternehmensstrategie ist. Dies ist in 52 Prozent der Unternehmen mit einer hohen Priorisierung für dieses Thema der Fall, aber nur in 23 Prozent der Unternehmen, die dem Thema eine geringe Priorität beimessen.

Abb. 12 – Cyber Security als Teil der Unternehmensstrategie



„Die Maßnahmen zur Vorsorge, aber auch im Cyber-Angriffsfall sind im Optimalfall in eine IT-Sicherheitsstrategie eingebettet. Diese beginnt mit einer Bewertung der unternehmenskritischen Anwendungen und endet mit Bereitschaftsregelungen und Backup-Strategien."

Norbert Weichele
Zentis GmbH & Co. KG



Eine enge Verzahnung der Unternehmensstrategie mit Maßnahmen der Cyber Security ist hier anzuraten. Dazu kann bspw. ein separates Information Security Management System (ISMS) etabliert werden, das mit anderen IT-Systemen wie der IT-Governance und IT-Compliance, aber auch den operativen Lösungen wie PPS- und ERP-Systemen abgestimmt sein muss. In der Studie (ohne eigene Abb.) nutzen nur 26 Prozent der Unternehmen ein separates ISMS, um die Cyber Security zu unterstützen.

Entsprechend zurückhaltend bewerten die teilnehmenden Mittelständler auch die Funktionsfähigkeit der eigenen Prozesse im Bereich Cyber Security (vgl. Abb. 13). Keiner der abgefragten Prozesse wird mehrheitlich als stark oder sehr stark funktionsfähig eingeschätzt. Reaktion auf, Vermeidung von sowie Erholung nach Cyber-Attacken erreichen je 38 Prozent. Noch schlechter schneiden die für ein erfolgreiches Management von Cyber-Risiken so wichtige Bewertung (32 Prozent) sowie die Identifikation (31 Prozent) ab.

Die Zuweisung der organisatorischen und prozessualen Verantwortung auf einen spezifischen Verantwortlichen kann sowohl unnötige Doppelarbeit vermeiden als auch an neuralgischen Punkten eine stärkere Überwachung sicherstellen. Hierfür bietet sich beispielsweise die Einrichtung einer speziellen Abteilung für Cyber Security im Unternehmen an.

„Um den Stellenwert von Cyber Security innerhalb von Unternehmen auf ein angemessenes Niveau zu heben, sollte die Verantwortlichkeit dafür ebenfalls bei den Unternehmensverantwortlichen liegen."

Alexander Iskender
IT-Verantwortlicher und Cyber-Experte

In der Stichprobe (vgl. Abb. 14) haben 50 Prozent der Unternehmen eine separate Fachabteilung für den Umgang mit Cyber-Risiken eingerichtet. In 30 Prozent liegt die organisatorische Verantwortung hingegen beim Datenschutzbeauftragten. Dies kann zwar in Einzelfällen sinnvoll sein. Im Normalfall ist dieser Entscheidungsträger jedoch bereits mit vielen anderen, nicht unbedingt nur mit Cyber Security verbundenen Themen beschäftigt und auch teilweise aus Kompetenzsicht nicht der richtige Ansprechpartner.

15 Prozent der Unternehmen haben auf der ersten oder zweiten Führungsebene die spezielle Position des Chief Information Security Officer (CISO) eingerichtet, um dem Thema einerseits eine noch höhere organisatorische Bedeutung einzuräumen und andererseits die teilweise verstreuten Anstrengungen im Unternehmen unter einer einheitlichen Leitung zu bündeln.

Abb. 13 – Funktionsfähigkeit von Prozessen

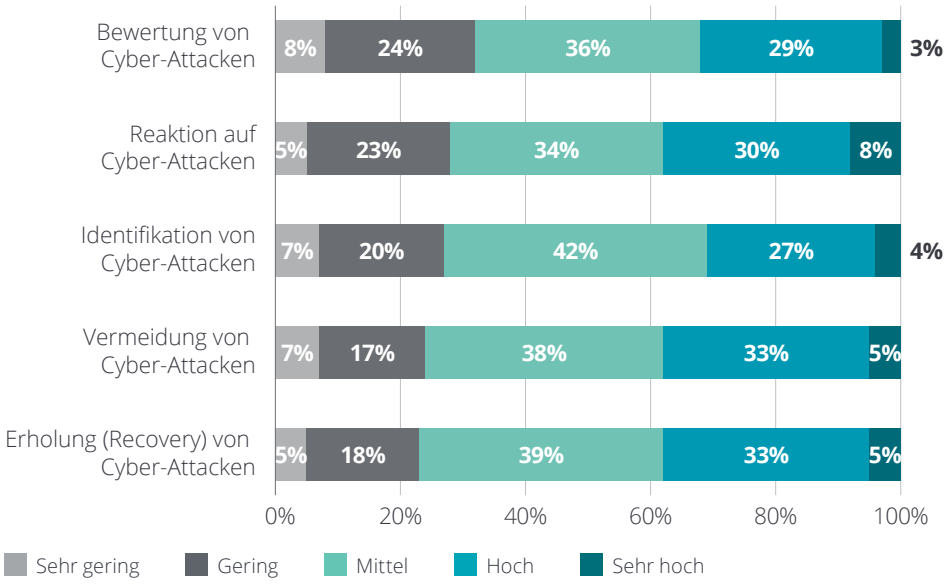
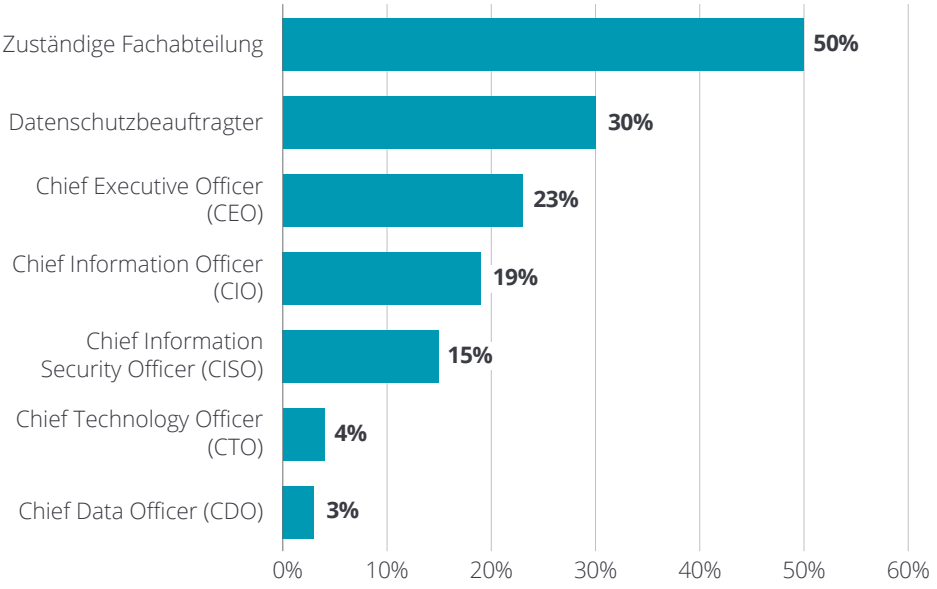


Abb. 14 – Existenz von spezifischen Verantwortlichen



Mitarbeiterperspektive

Für den Erfolg der Cyber-Abwehr wurde die überragende Bedeutung der Führungskräfte sowie technologischer und prozessualer Maßnahmen bereits deutlich. Zugleich wurden jedoch die Mitarbeiter immer wieder als Gefahrenherd identifiziert. In der Studie (vgl. Abb. 15) haben wir uns deshalb auch den Weiterbildungsmaßnahmen für Mitarbeiter im Bereich Cyber Security gewidmet. Prinzipiell sind hier sowohl interne Schulungen als auch Weiterbildungen durch externe Akteure wie Beratungsgesellschaften oder Strafverfolgungsbehörden denkbar. Das Schulungsniveau in den Unternehmen ist insgesamt gesehen noch eher niedrig, zudem wird weit häufiger intern als extern geschult. Intern werden in 45 Prozent der Fälle interne Gefahrensituationen, in 42 Prozent der Unternehmen das Thema Datenschutz und in 39 Prozent das Thema Data Security allgemein geschult. Bezogen auf externe Schulungen sind die Zahlen für Datenschutz 29 Prozent und Data Security allgemein 25 Prozent. Dass externe Trainer und Coaches weniger häufig auf spezifische interne Gefahren eingehen, war hingegen zu erwarten.

Die an der Studie teilnehmenden mittelständischen Unternehmen bewerten die Sensibilisierung der eigenen Mitarbeiter für im Bereich Cyber Security relevante Themen leider durchwegs als niedrig, was auf eine gefährliche Situation hindeutet (vgl. Abb. 16). Das Thema Datenschutz erhält mit 40 Prozent noch die höchste Zustimmung. Es folgen Internetsicherheit (39%), Passwortsicherheit (38%), Richtlinie zur Informationssicherheit, Identitätsmanagement und Phishing/Social Engineering (jeweils 28%), Cloud Security (25%), Sicherheit mobiler Datenträger (24%), Sicherheit mobiler Endgeräte (19%) sowie Informationsklassifizierung (17%).

Es entsteht also durchaus der Eindruck, dass die Fachmitarbeiter im Mittelstand für viele der von Cyber-Attacken ausgehenden Gefahren nicht hinreichend sensibilisiert sind, was zu konkreten Risikosituationen führt.

„Die beste Cyber-Security-Technik nützt nicht viel, wenn die Mitarbeiter eines Unternehmens im Fokus der Attacke stehen. Daher ist es ratsam, neben technischen Maßnahmen in jedem Falle auch begleitende Awareness-Maßnahmen umzusetzen. Insbesondere die Themen (Spear-)Phishing und Social Engineering sollten dabei im Fokus stehen. Es gilt folgender Grundsatz: 1. Technik so sicher wie möglich machen 2. Security-Awareness sicherstellen."

Moritz Huber
LKA Baden-Württemberg

Abb. 15 – Weiterbildungsmaßnahmen für Mitarbeiter im Unternehmen

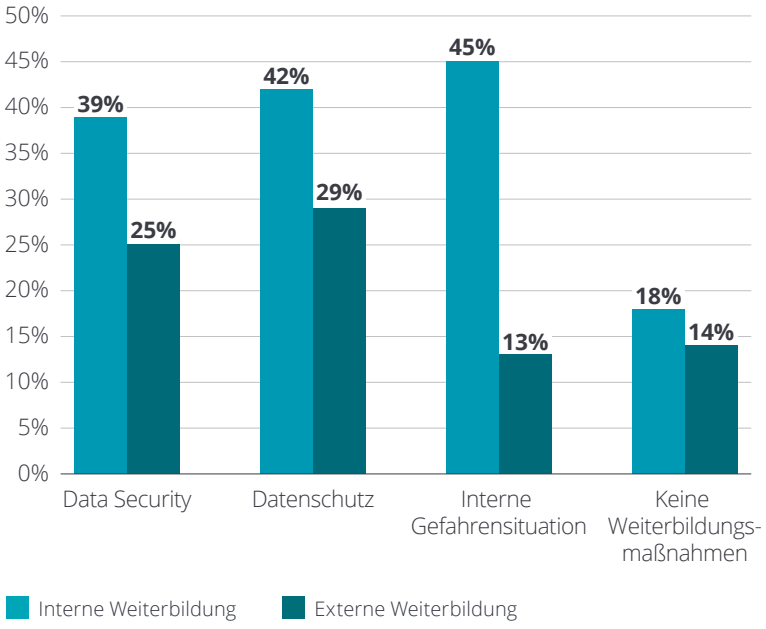
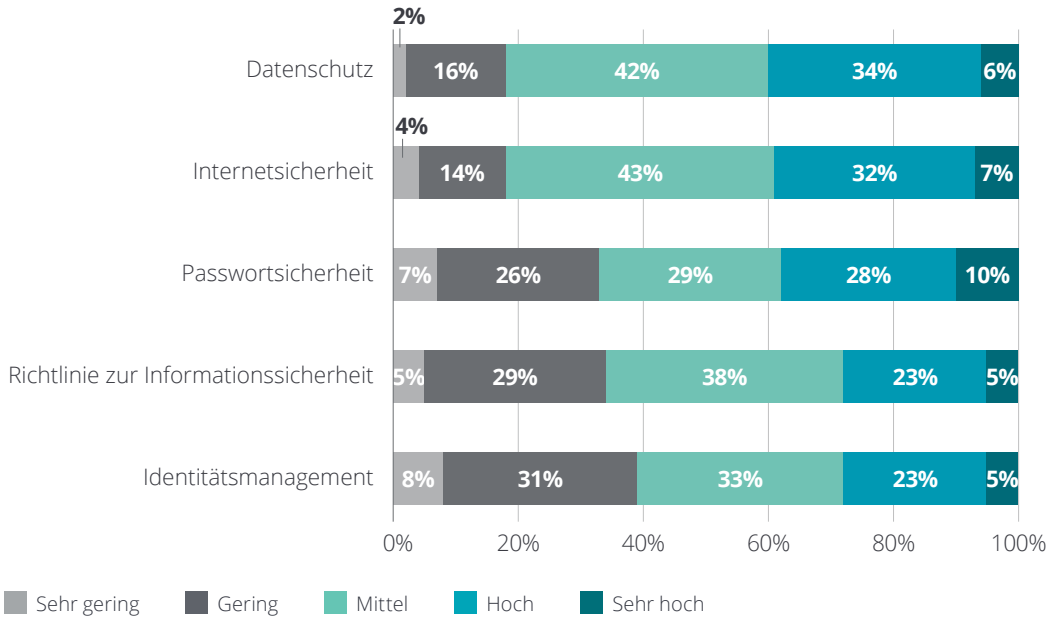


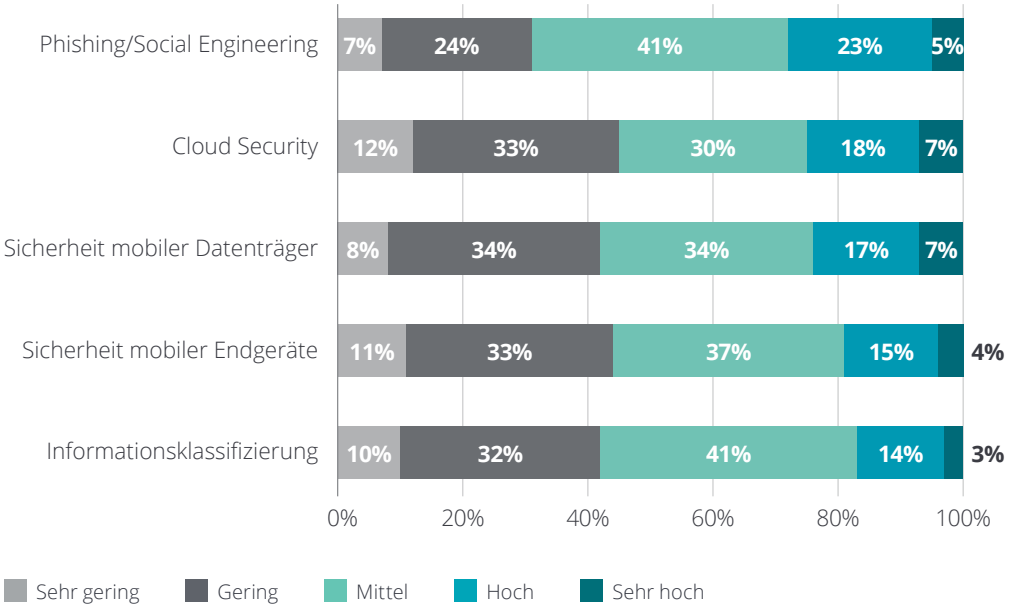
Abb. 16 – Sensibilisierung der Mitarbeiter (Teil I)



„Die Herausforderungen der Cyber Security müssen bereits bei der Auswahl von Systemen betrachtet werden (‚Security by Design'). Dieses Thema kann ein Mittelständler jedoch nicht allein lösen. Er muss sich in größere Strukturen oder Plattformen integrieren. In diesem Kontext sind bisher keine weitreichenden europäischen Lösungen erkennbar. Aktuell sind nur amerikanische oder chinesische Plattformen zu sehen. Wer kann diese Lücke schließen?"

Norbert Weichele
Zentis GmbH & Co. KG

Abb. 17 – Sensibilisierung der Mitarbeiter (Teil II)



In diesem Kapitel haben wir uns konkreten Bedrohungs- und Verlustszenarien und den Reaktionen des Mittelstands gewidmet. Es wurde ein zunehmendes Auseinanderdriften von der Bedrohungslage konkreter Attacken und nicht hinreichender organisatorischer sowie mitarbeiterbezogener Vorbereitung deutlich. In vielen Unternehmen wird Erstere schlichtweg unterschätzt oder zumindest nicht realistisch bewertet. Neben organisatorischen Maßnahmen und Weiterbildungen für Mitarbeiter können zwar Versicherungen den Schutz mittelständischer Unternehmen gegen Cyber-Attacken nicht grundsätzlich erhöhen, aber vornehmlich die finanziellen Folgen abmildern.

„Nachlässigkeit und Unkenntnis auf dem Gebiet der Cyber-Sicherheit können in zunehmendem Maße eine Gefahr für Leib und Leben darstellen. Denken wir nur an Sicherheitslücken, die bereits in Herzschrittmachern und Insulinpumpen aufgetreten sind und eine Fernsteuerung durch Unbefugte ermöglichten. Ferner OP-Roboter, die aus dem Internet ungeschützt erreichbar waren. Oder die Daten ganzer Krankenhäuser, die von Ransomware verschlüsselt wurden."

Prof. Dr. Roland Hellmann
Hochschule Aalen

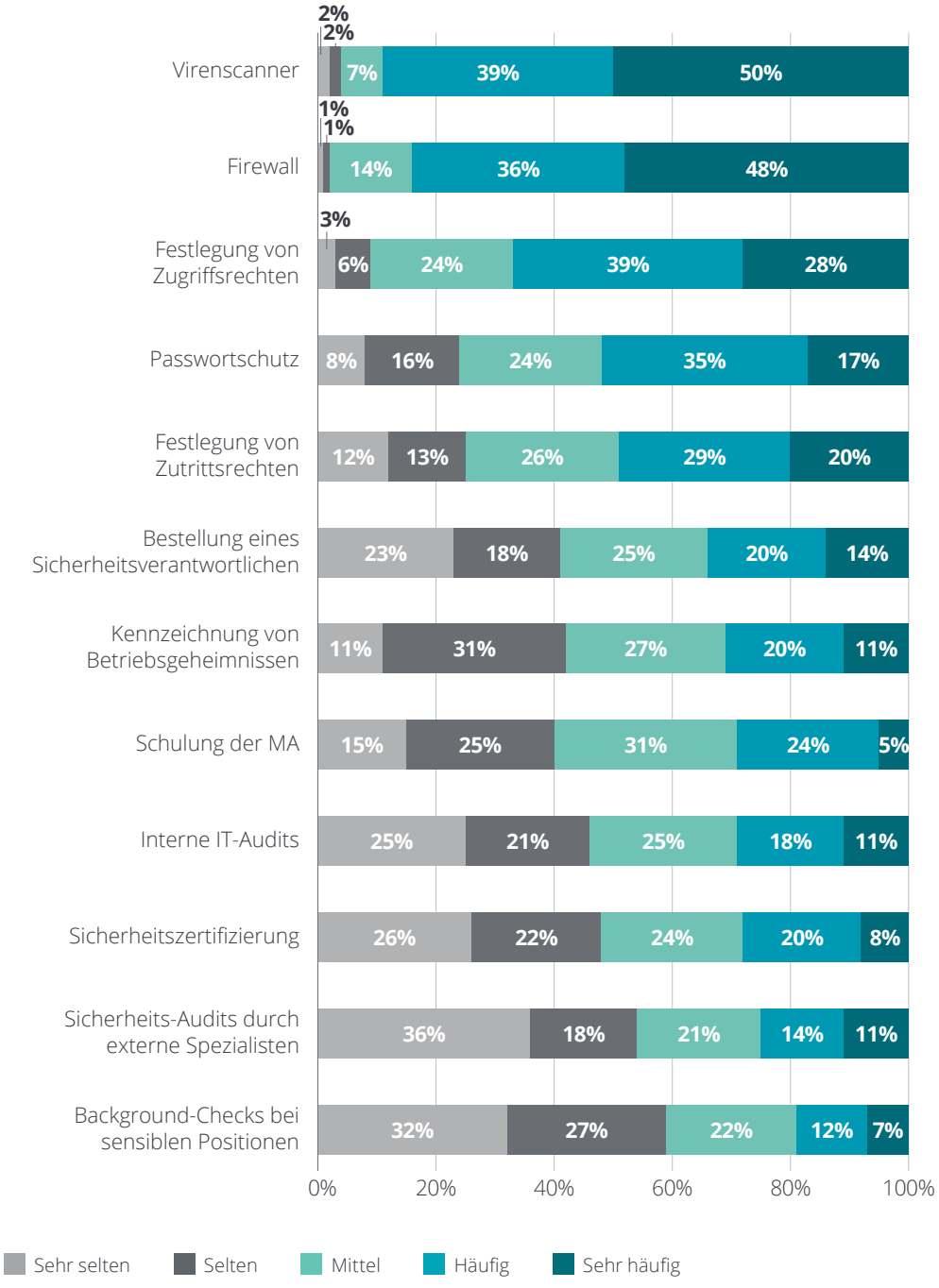
III. Budget und Cyber-Versicherungen – welche konkreten Pläne hat der Mittelstand?

Maßnahmen zur Verbesserung der Abwehrfähigkeit gegen Cyber-Attacken sind für mittelständische Unternehmen zeitlich aufwendig, benötigen Personal und natürlich auch ein entsprechendes Cyber-Budget. In der Regel lohnen sich die Investments jedoch, denn die direkten sowie indirekten finanziellen und sonstigen Schäden (z.B. Vertrauens- und Reputationsverlust in der Öffentlichkeit) übersteigen die primären Ausgaben meist um ein Vielfaches. Für den Mittelstand ergibt sich aber – anders als für die meisten Großunternehmen – die Situation, dass die finanziellen Mittel stärker beschränkt sind und dass die Verantwortlichen für Cyber Security mit anderen Entscheidern um Budgets konkurrieren. Zudem ist der direkte Nutzen von Cyber-Maßnahmen asymmetrisch erst im Schadensfall zu erkennen und wird deshalb von Entscheidern meist unterschätzt, während der Nutzen marktwirksamer Ausgaben wie z.B. für Marketing und Strategien hingegen überschätzt wird. Umso wichtiger ist es, für die Notwendigkeit von Maßnahmen zur Steigerung der Abwehr- und Reaktionsfähigkeit gegen Cyber-Attacken im Mittelstand zu sensibilisieren.

Maßnahmen und Kosten für Cyber Security

In der Studie (vgl. Abb. 18) haben wir zunächst abgefragt, welche konkreten Maßnahmen die Unternehmen im Bereich Cyber Security umsetzen. 89 Prozent der Studienteilnehmer greifen häufig oder sehr häufig auf Virenscanner zurück. Auch Firewalls werden in 84 Prozent der Unternehmen häufig eingesetzt. Es folgen die Festlegung von Zugriffsrechten (67%), Passwortschutz (52%) und die Festlegung von Zutrittsrechten (49%). Weitere Aspekte wie die Bestellung eines Sicherheitsverantwortlichen, die Schulung von Mitarbeitern, Sicherheits-Zertifizierungen oder externe Sicherheits-Audits werden schon nur noch von einer deutlichen Minderheit der Unternehmen häufig eingesetzt. Gerade letztere Maßnahme nutzen nur 25 Prozent der Teilnehmer. Einige der befragten Experten berichten hingegen von Einzelfällen, in denen eigens mit einem Sicherheits-Audit beauftragte Spezialisten Systeme auch größerer Unternehmen häufig innerhalb weniger Minuten nicht nur penetrieren, sondern sogar übernehmen konnten – eine beängstigende Vorstellung.

Abb. 18 – Maßnahmen für Cyber Security



Einen hundertprozentigen Schutz gegen Cyber-Attacken bieten auch diese Maßnahmen leider nicht. Um die Risiken jedoch weitgehend einzuschränken und beherrschbar zu machen, können mittelständische Unternehmen selbst etwas tun. Das BSI hat beispielsweise sogenannte Kernmaßnahmen sowie ergänzende Maßnahmen veröffentlicht, die nicht nur Privatpersonen, sondern auch Unternehmen einen ersten Anhaltspunkt bieten können. Zu den Kernmaßnahmen gehören Aspekte wie aktuelle Software, Virenschutz und Firewall, Benutzerkonten und Rechteverwaltung sowie Zurückhaltung bei der Weitergabe persönlicher Daten. Hier wird bereits klar, dass Systeme wie Mitarbeiter gleichermaßen gefordert sind. Im Rahmen der ergänzenden Maßnahmen haben sich v.a. Verfehlungen bei den Themen Datenverschlüsselung sowie mangelnde Vorsicht beim Umgang mit E-Mails und Anhängen in den letzten Monaten als ursächlich für erfolgreiche Cyber-Attacken erwiesen.

Wir haben Unternehmen und Experten in der Studie auch danach befragt, wie viel sie pro Jahr für Cyber Security als Budget veranschlagen. Unsere Praxiserfahrung sagt uns, dass ca. zwischen 5 und 20 Prozent der IT-Kosten eines Unternehmens als Größenordnung für das Cyber-Budget realistisch sind. Anteilig am Umsatz sind dies meist 0,5 bis 2 Promille (die Cyber-Kosten machen ca. 10 Prozent der IT-Kosten aus). Übertragen wir dies auf unsere Stichprobe, müssten die Unternehmen bei einem Umsatz-Mittelwert von 387 Mio. Euro zwischen 193.500 und 774.000 Euro pro Jahr für Cyber Security ausgeben. Auch wenn dies natürlich nur eine Mittelwertbetrachtung ist, zeigt unsere Studie (vgl. Abb. 19), dass 89 Prozent der Unternehmen diese Anforderung nicht erfüllen. Nur 10 Prozent der Befragten geben über 100.000 Euro pro Jahr für Cyber Security aus. Der entsprechende jährliche Mittelwert in unserer Studie beläuft sich auf 80.050 Euro.

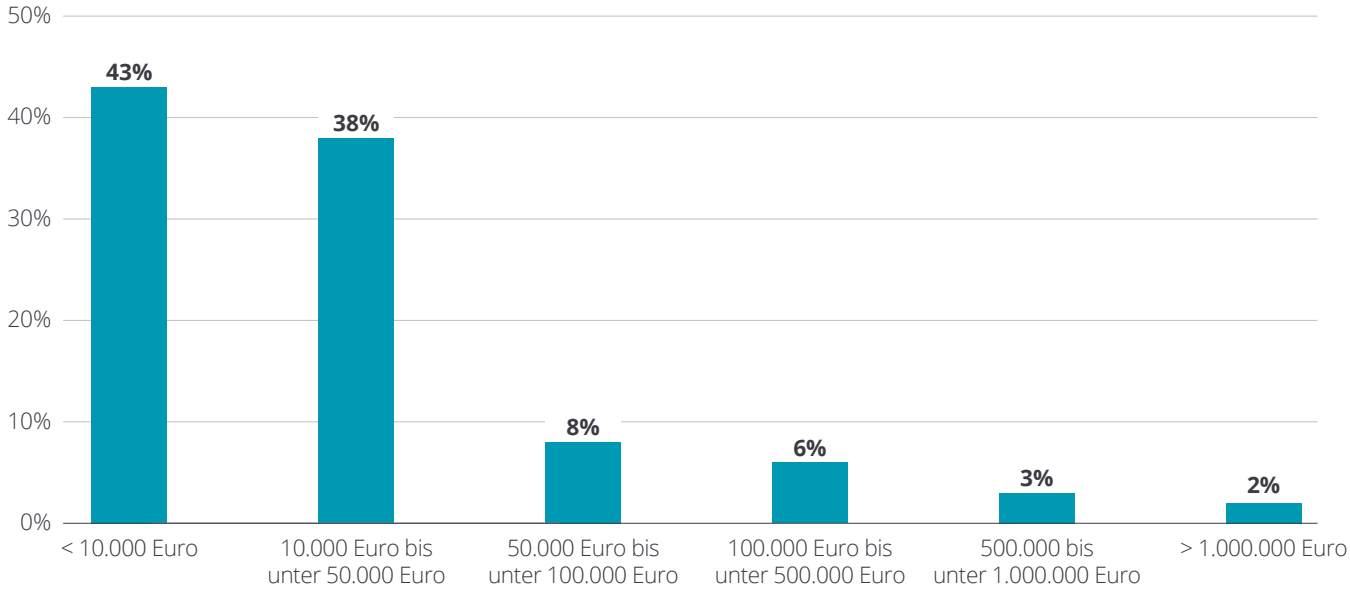
„Es standen schon Wasserkraftwerke, Ampelanlagen, Seilbahnen und Säurepumpen von Swimmingpools ungeschützt im Internet. Unbefugte hätten sie nach Belieben manipulieren können, und das von jedem Ort der Erde aus. Und wie kam es dazu? Probleme waren häufig unsichere Default-Konfiguration und mangelnde Absicherung am Ort der Installation. Geräte und Software werden in Betrieb genommen, ohne die Dokumentation zu beachten. Und Anlagen, die nie dafür gedacht waren, hängen plötzlich am Internet."

Prof. Dr. Roland Hellmann
Hochschule Aalen

„Der Mittelstand ist besonders stark von gezielten Cyber-Attacken bedroht. Mittelständische Unternehmen verfügen häufig über technisches Know-how, welches für Angreifer ein erstrebenswertes Ziel darstellt. Gleichzeitig berücksichtigen viele Unternehmen nicht die beispielsweise vom BSI empfohlenen Standards für Cyber Security. Oft steht kein ausreichendes Budget zur Verfügung, um den Herausforderungen, welche die Risiken von Cyber-Attacken mit sich bringen, ausreichend zu begegnen."

Alexander Iskender
IT-Verantwortlicher und Cyber-Experte

Abb. 19 – Jährliche Ausgaben für Cyber Security



„Cyber Security ist für Unternehmen ein wesentlicher Kostenfaktor. Budget, das in die Sicherheit von Netzwerken, Datenbanken und Systemen investiert wird, steht an anderer Stelle – beispielsweise für Produktentwicklung und Marketing – nicht mehr zur Verfügung. Vor diesem Hintergrund besteht der Anreiz, das Risiko, das von Cyber-Attacken für das Unternehmen ausgeht, möglichst niedrig anzusetzen, um die Kosten in diesem Bereich überschaubar zu halten."

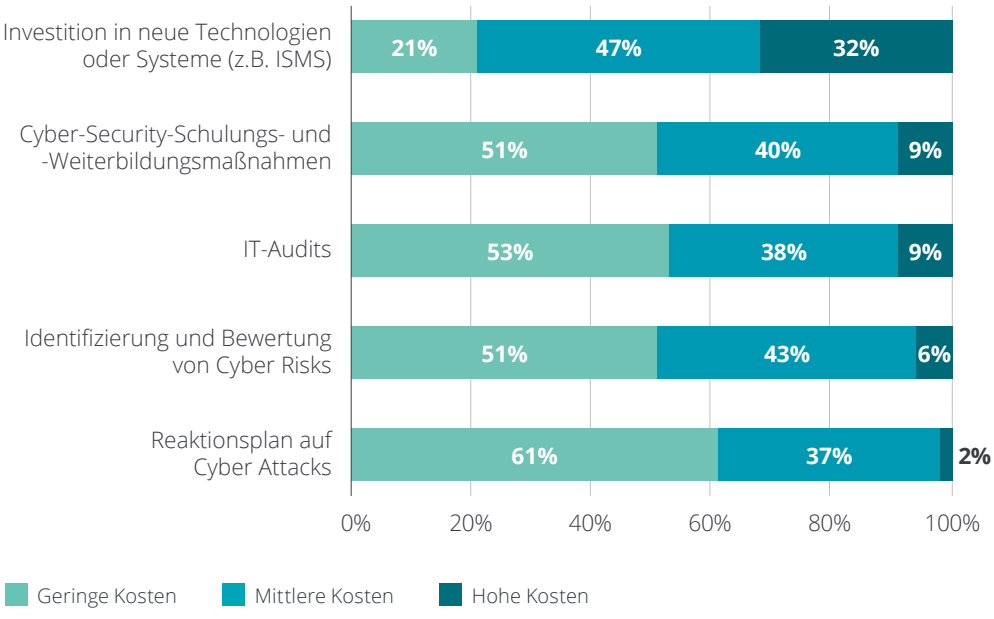
Alexander Iskender
IT-Verantwortlicher und Cyber-Experte

Eine zusätzliche Frage (ohne eigene Abb.) ergab, dass 51 Prozent der Unternehmen trotz erhöhter Sensibilisierung für das Thema keine zusätzlichen Ausgaben für die nächsten Jahre einplanen.

Die Studie (vgl. Abb. 20) zeigt die Verteilung der Kosten auf verschiedene Kategorien. 79 Prozent der Befragten planen für neue Technologien und Systeme hohe oder sehr hohe Kosten ein. Es folgen Schulungs- und Weiterbildungsmaßnahmen (49%), Identifikation und Bewertung von Cyber-Risiken (49%), IT-Audits (47%) sowie Reaktionspläne für Cyber-Attacken (39%).

Neben konkreten operativen Maßnahmen wurde zuletzt auch stärker die Sinnhaftigkeit von Versicherungen gegen Cyber-Risiken diskutiert. Deshalb gehen wir auf diesen Themenbereich separat ein.

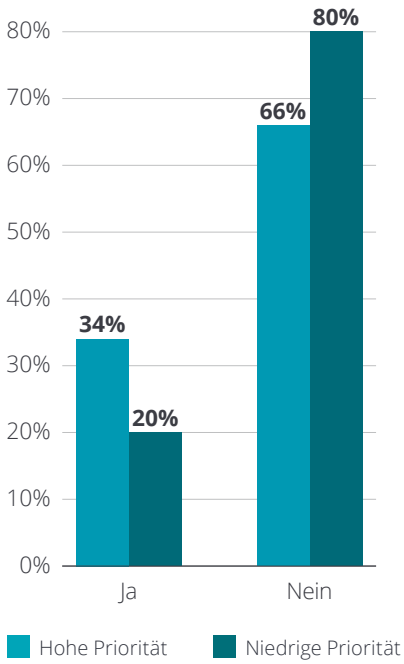
Abb. 20 – Verteilung der Kosten



Sinnhaftigkeit und konkrete Möglichkeiten von Versicherungslösungen

Die Cyber-Versicherung ist eine Möglichkeit für mittelständische und Großunternehmen, Eigen- und Drittschäden im Zusammenhang mit Hackerangriffen oder sonstigen Handlungen in Zusammenhang mit Cyber-Kriminalität je nach individueller Vereinbarung zu versichern. Zwar kann die Cyber-Versicherung Aspekte wie bspw. Reputationsschäden nicht absichern, jedoch einen gewissen Schutz bzgl. der möglichen direkten und indirekten Vermögensschädigungen geben.

Abb. 21 – Vorhandensein einer Cyber-Versicherung



„Unternehmen können sich inzwischen sehr gut gegen Cyber-Attacken versichern. Für mittelständische Unternehmen bieten ca. 25 Gesellschaften Cyber-Konzepte an. Versichert werden können Eigenschäden, insbesondere Wiederherstellungskosten und Betriebsunterbrechungen nach Cyber-Vorfällen. Der Assekuranzschutz beinhaltet auch Bedienfehler von Mitarbeitern. Optional versichert werden können auch Schäden als Folge von technischen Problemen. Daneben sind Datenschutzvorfälle, Erpressungen, aber auch Fremdschäden (Haftung des Unternehmens) vom Versicherungsschutz umfasst."

Erich Burth
RVM Versicherungsmakler GmbH & Co. KG

Prinzipiell können Cyber-Versicherungen Eigen- und Fremdschäden abdecken. Hierzu gehören bspw. Aspekte wie die Kosten für die Wiederherstellung von Daten und IT-Systemen, PR-Maßnahmen, Kosten infolge einer Betriebsunterbrechung, solche für forensische Untersuchungen und die für spezialisierte Cyber-Anwälte. Zu den Fremdschäden, die in der Praxis mehrheitlich Vermögensschäden darstellen, gehören Schadenersatzforderungen von Geschäftspartnern und Kosten, die in der Folge der Verletzung von Vertragspflichten (z.B. Geheimhaltung) entstehen.

In der Studie (ohne eigene Abb.) haben nur 28 Prozent der Unternehmen eine solche Versicherung abgeschlossen. Die Kontrastierung nach Cyber-Priorität (vgl. Abb. 21) ergibt, dass in der Gruppe der Unternehmen mit höherer Sensibilisierung 34 Prozent, in der Gruppe mit niedriger Priorität nur 20 Prozent eine solchen Versicherung abgeschlossen haben. Bei den Befragten mit einer solche Versicherung (ohne eigene Abb.) deckt diese zu 84 Prozent Eigenschäden, zu 82 Prozent Fremdschäden und zu 57 Prozent Serviceleistungen ab.

In diesem Kapitel haben wir gesehen, welche konkreten Maßnahmen mittelständische Unternehmen gegen Cyber-Attacken durchführen können und dass diese auch ein gewisses finanzielles Budget benötigen. Gleichzeitig können sie jedoch keine Sicherheitsgarantie abgeben. Zudem haben wir diskutiert, dass Cyber-Versicherungen die Absicherung gegen finanzielle Folgen einer Cyber-Attacke erhöhen können.

Nach dem Interview mit Erich Burth auf den nächsten Seiten wollen wir im darauffolgenden Kapitel einen Ausblick auf offene Handlungsfelder im Mittelstand geben.

„Cyber-Versicherungen bringen zusätzliche Vorteile: Das notwendige Assessment für den Abschluss der Versicherung ermöglicht ein Benchmark zum Status der vorbeugenden Maßnahmen. Zudem können die Risiken und die vorbeugenden Maßnahmen besser bepreist werden."

Norbert Weichele
Zentis GmbH & Co. KG

Interview mit dem Versicherungsexperten Erich Burth

Zur Verifikation der in der Studie thematisierten Bereiche haben wir ein Gespräch mit dem Cyber-Versicherungsexperten Erich Burth geführt. Er ist Geschäftsführender Gesellschafter der RVM Versicherungsmakler GmbH & Co. und auf die Beratung zu Cyber-Versicherungen spezialisiert.

Von welchen Quellen (Stichworte Hacker, Insider) gehen für mittelständische Unternehmen die größten Sicherheitsrisiken aus?

Die mit Abstand häufigste Schadenursache im Mittelstand ist der Befall mit einer Ransomware, d.h. einem Verschlüsselungstrojaner. Stark zugenommen haben aber auch Datenschutzvorfälle und Gefährdungen durch kompromittierende geschäftliche E-Mails, die dann die IT-Systeme außer Funktion setzen. Eine erhebliche Rolle spielen auch Fälle bewusster Sabotage. Diese sind zwar nicht sehr häufig, verursachen aber sehr hohe Schäden. DDoS-Attacken (Distributed-Denial-of-Service-Attacken; Überlastung von Internetnetzen) sind eher selten, diese treffen häufig größere Unternehmen.

Wird die menschliche Komponente (Mitarbeiterverhalten) im Bereich Cyber Security unterschätzt?

Inzwischen ist den Kunden bewusst, dass menschliches Verhalten eine große Rolle für die Verhinderung von Cyber-Schäden spielt. Menschliches Verhalten in den betroffenen Unternehmen ist nach Statistiken der Versicherer für über 40 Prozent aller Schadenfälle ursächlich (vgl. Hiscox Cyber Readiness Report 2019). Das Bewusstsein hierfür ist aber gerade im letzten Jahr ebenfalls deutlich gewachsen. Inzwischen werden Mitarbeiter häufiger regelmäßig geschult im Umgang mit Mailverkehr oder Phishing-Attacken. Entgegen der Empfehlung ihrer Unternehmen verwenden Mitarbeiter dennoch häufig „schwache" Passwörter und/oder nutzen ein Passwort für mehrere Anwendungen. In mittelständischen Unternehmen werden die (oft vorhandenen) entsprechenden Vorgaben oft auch nicht stringent umgesetzt und überwacht. Im AIG Schadenreport 2019 haben sich die Schadenmeldungen wegen Fahrlässigkeit von Mitarbeitern von 7 auf 14 Prozent verdoppelt. Die Schäden werden dadurch ausgelöst, dass Mitarbeiter E-Mails mit Unternehmensdaten an falsche Adressaten senden oder Laptops und andere technische Geräte verlieren. Außerdem hat seit Inkrafttreten der DSGVO die Zahl der Meldungen solcher Vorfälle zugenommen.

Welche konkreten Risiken (z.B. mobile Endgeräte, Social Media, Phishing) halten Sie im Mittelstand für besonders relevant?

Im Mittelstand sind Schäden durch den Faktor Mensch besonders ausgeprägt, d.h., kompromittierende E-Mails oder andere Phishing-Attacken haben eine besondere Bedeutung (s.a. die Antwort auf die zweite Frage).

Wie sieht aus Ihrer Sicht ein effektiver und effizienter Maßnahmen- und Notfallplan im Fall einer Cyber-Attacke aus?

Die Kunden sollten einen solchen Fall durchgespielt und im Idealfall auch geübt haben. Wichtig ist, dass die Verantwortlichkeiten klar geregelt sind und die Ansprechpartner auch erreicht werden können, ohne dass die IT-Landschaft funktioniert. Ferner sollte bekannt sein, welche externen Experten zur Unterstützung angesprochen werden können. Hierbei ist der Abschluss einer Cyber-Versicherung sehr hilfreich, weil die Versicherer über entsprechende Ressourcen verfügen.

Kann und sollte man sich gegen Cyber-Attacken versichern? Wie teuer ist das? Was sind die Voraussetzungen?

Unternehmen können sich inzwischen sehr gut gegen Cyber-Attacken versichern. Für mittelständische Unternehmen bieten ca. 25 Gesellschaften Cyber-Konzepte an. Versichert werden können Eigenschäden, insbesondere Wiederherstellungskosten und Betriebsunterbrechungen nach Cyber-Vorfällen. Der Assekuranzschutz beinhaltet auch Bedienfehler von Mitarbeitern. Optional versichert werden können auch Schäden als Folge von technischen Problemen. Daneben sind Datenschutzvorfälle, Erpressungen, aber auch Fremdschäden (Haftung des Unternehmens) vom Versicherungsschutz umfasst. Von besonderer Bedeutung gerade für mittelständische Unternehmen sind die Unterstützungsleistungen der Versicherer im Schadenfall (IT-Forensik, Rechts- und Krisenberatung). Die Prämien sind noch vergleichsweise günstig. So würde ein Produktionsbetrieb mit ca. 100 Mio. Euro Umsatz bei einer Deckungssumme von 3 bis 5 Mio. Euro eine Prämie von ca. 5.000 bis 10.000 Euro bezahlen müssen. Voraussetzung für eine Deckung ist das Einhalten der Mindeststandards der IT-Sicherheit (Firewalls, Virenscanner, ausreichender Passwort-Schutz, mindestens wöchentliche Datensicherung).

Wo sehen Sie im Bereich Cyber Security im Mittelstand die größten Handlungsbedarfe?

Im Etablieren übergreifender Verantwortlichkeiten und in der Umsetzung der vereinbarten Maßnahmen im Unternehmen. Wichtig sind auch die Einführung eines kontinuierlichen Verbesserungsprozesses und das Aufbauen eigener Kompetenzen zum Cyber-Risiko mit der Festlegung technisch-organisatorischer Maßnahmen inkl. der Auswahl geeigneter IT-Dienstleister. Das Risikobewusstsein der Belegschaft muss gefördert werden, um die „Schwachstelle Mensch" weitestgehend zu entschärfen.

Wie viel sollte man für Cyber Security pro Jahr ausgeben, damit man gut geschützt ist?

Diese Frage lässt sich so allgemein schwer beantworten. Die Gefährdung hängt stark vom Stand der Digitalisierung und der Branche des jeweiligen Unternehmens ab. Ferner ist IT-Sicherheit oft Bestandteil anderer Budget-Posten (IT-Administration, Software-Einkauf, Datenschutz etc.). Wir sehen für das IT-Budget eine Range von 0,5 bis 3 Prozent vom Umsatz als realistische Größenordnung.

IV. Ein Blick in die Zukunft – quo vadis Mittelstand?

Cyber Security ist aktuell in aller Munde. Nicht nur das BSI, sondern alle in diesem Bereich aktiven Organisationen und Einzelpersonen gehen davon aus, dass die Bedrohungslage und damit die Anzahl versuchter und erfolgreicher Attacken in den Folgejahren noch deutlich zunehmen werden. Dies ist in der immer weiter ansteigenden digitalen Vernetzung der Weltwirtschaft begründet.

„Die Anforderungen an die Cyber Security wandeln sich mit zunehmender Digitalisierung. Die ‚Industrie 4.0' stellt auch den Mittelstand vor neue Herausforderungen. Über Cloud-Systeme und den Einsatz von mit dem Internet verbundenen Geräten und Maschinen (Stichwort IoT) ist es nicht mehr möglich, Systeme vollständig nach außen abzuschotten. Mit zunehmender Vernetzung von Produktions- und Kommunikationsprozessen erhöhen sich die Anzahl potenzieller Angriffspunkte und das Spektrum der Angriffsarten. Die Software-Entwicklungszyklen verkürzen sich dadurch signifikant, Sicherheitslücken müssen umgehend geschlossen werden."

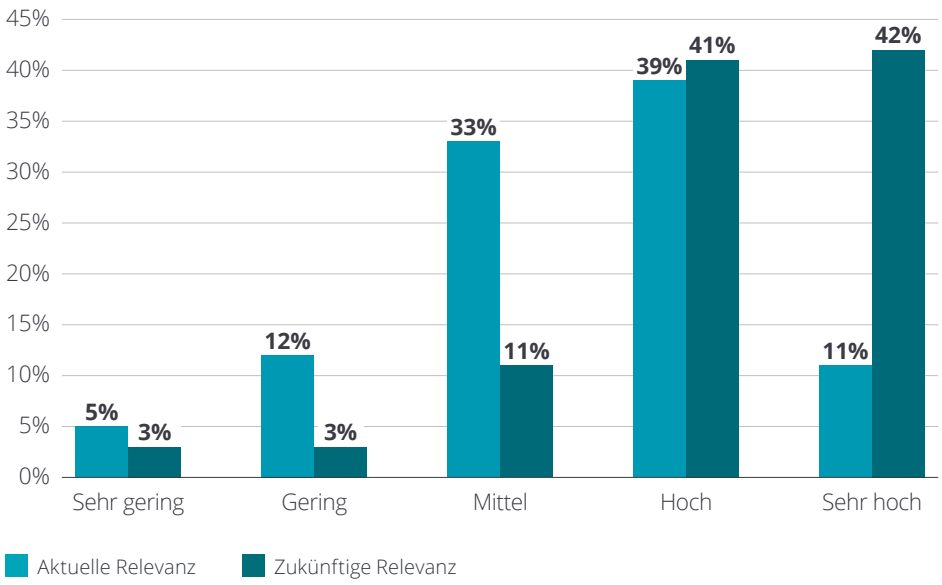
Alexander Iskender
IT-Verantwortlicher und Cyber-Experte

Doch wie sehen das die in unserer Studie befragten Unternehmen? Ein Vergleich der aktuellen mit der zukünftigen Relevanz (vgl. Abb. 22) zeigt hier zumindest ein stark ansteigendes Problembewusstsein: Der Anteil der Unternehmen, die dem Thema eine sehr hohe Relevanz zuweisen, steigt von 11 auf 42 Prozent.

„Der größte Handlungsbedarf liegt im Bereich der Erkennung von Attacken, da auftretende Anomalien erkannt und analysiert werden müssen, bevor es zu einer Reaktion auf Cyber-Angriffe kommen kann."

Ralph Noll
Deloitte

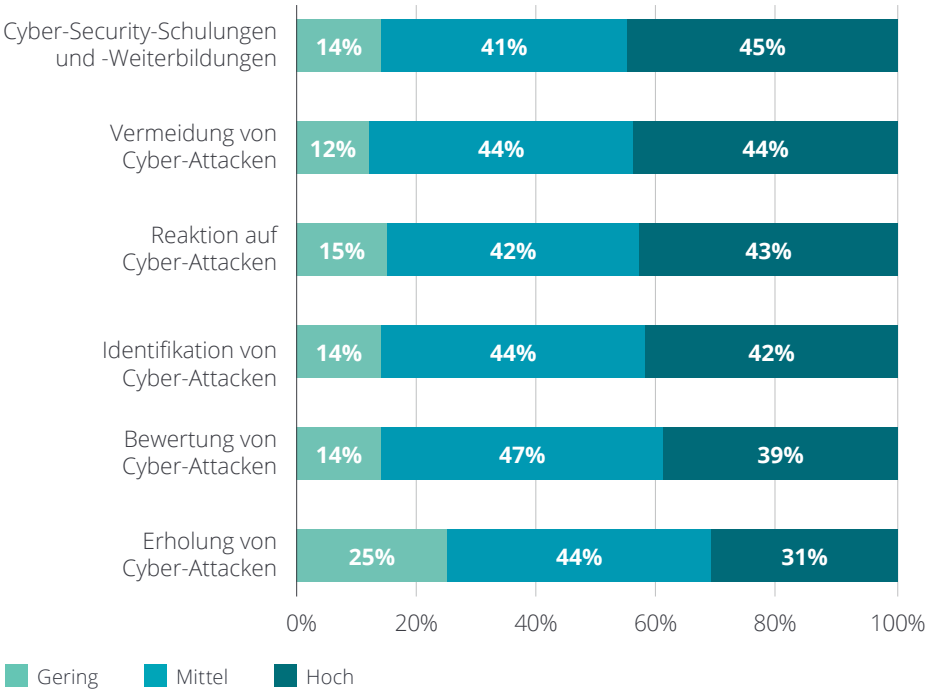
Abb. 22 – Aktuelle und zukünftige Relevanz von Cyber Security



Ebenfalls von Interesse ist die Frage, welche konkreten Verbesserungspotenziale Unternehmen und Experten für den Mittelstand entdeckt haben. Diese Aspekte haben wir in Abbildung 23 ausgewertet. Hier zeigen sich über die gesamte Stichprobe hinweg bei ca. 50 Prozent der Befragten Nachholbedarfe in sämtlichen für Cyber Security relevanten Bereichen. Das größte Defizit erkennen die Unternehmen in Bezug auf Schulungen und Weiterbildungen (45%). Weiterhin werden die Vermeidung von (44%), die Reaktion auf (43%) und die Identifikation von Cyber-Attacken (42%), deren Bewertung (39%) und – etwas geringer – die Erholung nach solchen Angriffen (31%) genannt. Letzterer Aspekt kann jedoch auch daran liegen, dass im Mittelstand bisher quantitativ erst eine geringere Zahl erfolgreicher Attacken durchgeführt wurde.

Unsere Studie hat Möglichkeiten und Potenziale, aber auch Gefahren und Risiken der Cyber Security in mittelständischen Unternehmen aufgezeigt. Das Problembewusstsein hat in den letzten Wochen und Monaten stark zugenommen, jedoch entsprechen Awareness, Sensibilisierung, konkrete Maßnahmen und Budgets im Mittelstand noch nicht immer dem wünschenswerten Stand. Hier sind durch Forscher, Unternehmen, Berater und Sicherheitsbehörden in der Zukunft weitere Anstrengungen zur Erhöhung der Cyber-Sicherheit des deutschen Mittelstands zu leisten.

Abb. 23 – Konkrete Verbesserungspotenziale



„Nach manchen Schätzungen liegt mehr als die Hälfte des Unternehmenswertes in seinen Daten. Wem vertraut man sein halbes Unternehmen an? Und wie erhält man diese Werte auf Dauer?“

Prof. Dr. Roland Hellmann
Hochschule Aalen

Empfehlungen für die Praxis

Awareness für das Thema Cyber Security schaffen

Aufgrund der speziellen Situation des Mittelstands, der sich durch eine tradierte Belegschaftsstruktur, zugleich aber hoch innovative Geschäftsmodelle und für Angreifer lukrative Ziele auszeichnet, bewegen sich Unternehmen in einem ungünstigen Spannungsfeld. Gerade vor dem Hintergrund der Tatsache, dass im Grundsatz bereits eine einzige Sicherheitslücke oder ein einzelner menschlicher Fehler Unternehmenssysteme dauerhaft kompromittieren kann, kommt der Information und Kommunikation von durch Cyber-Attacken ausgehenden Gefahren gegenüber den Mitarbeitern eine überragende Bedeutung zu. Neben der passiven Information können aktive Übungen wie Awareness-Trainings, Red Teaming und War Gaming die Achtsamkeit für das Thema in Unternehmen weiter erhöhen.

Die Faktoren Technologie und Mensch gleichermaßen berücksichtigen

Wie viele andere Themen in Unternehmen auch wird Cyber Security aktuell noch zu häufig in organisatorischen Silos betrachtet und zudem oft als rein technische Herausforderung für IT-Experten gesehen. Beide Aspekte sind durchaus problembehaftet: Der Mittelstand hat einerseits meist nicht die finanziellen Kapazitäten, um sich für jedes sicherheitsrelevante Thema Experten zu leisten. Andererseits führt die Zuschreibung der Verantwortung für Cyber Security zur IT bei vielen Nicht-IT-Mitarbeitern zu einer gewissen Sorglosigkeit im eigenen Verhalten. Hinzu kommt: Nur wenige IT-Spezialisten sind gleichzeitig IT-Sicherheits-Spezialisten. Neben der Einführung übergreifender Systeme wie eines Informationssicherheitsmanagementsystems (ISMS) kann hier die Einrichtung der organisatorischen Position eines CISO (Chief Information Security Officer) die Aktionsfähigkeit der Unternehmen stark erhöhen.

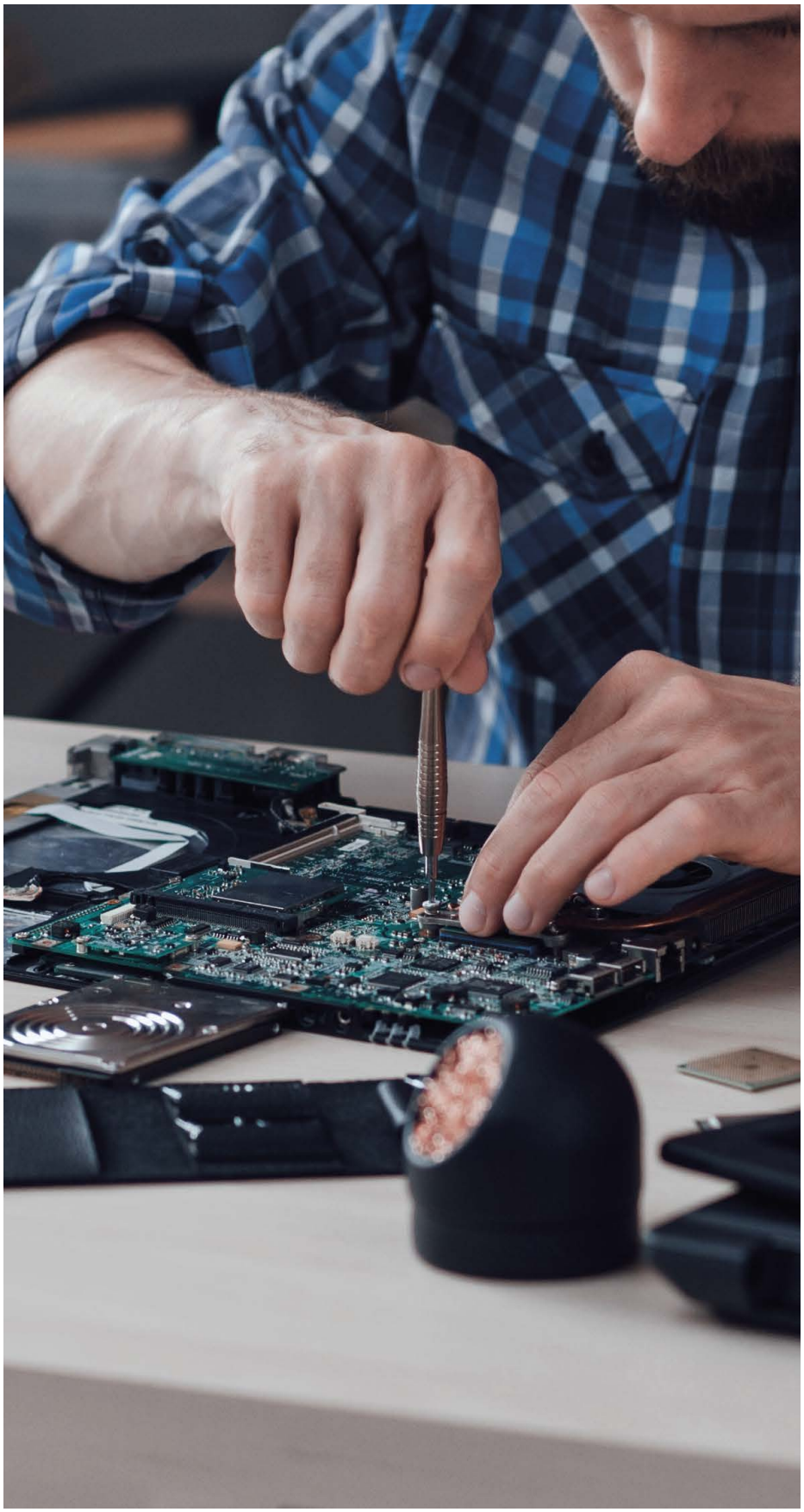
Organisatorische Verantwortlichkeiten klären und Notfallpläne etablieren

Anknüpfend an das Spannungsfeld Mensch vs. Maschine sind organisatorische Verantwortlichkeiten sowie Rollen im Cyber-Security-Abwehrprozess häufig nicht klar

definiert. Insbesondere die Fachbereiche Compliance, IT/EDV sowie Digitalisierung (falls voneinander getrennt) haben ggf. konkurrierende oder sich überschneidende Verantwortlichkeiten. Sicherlich lässt sich dies in der Praxis nicht vollständig vermeiden und eine gewisse Doppelarbeit ist bisweilen sogar positiv. Im Fall eines gelungenen Angriffs zeigen Studien jedoch, dass eine erfolgreiche Abwehr von klaren Rollen, konzertierten Aktionen, dem Vorhandensein und der klaren Umsetzung von Notfallplänen sowie nicht zuletzt von finanziellen Reserven zur Überbrückung etwaiger Problemphasen profitiert.

Realistisch investieren und Versicherungsmöglichkeiten prüfen

Experten gehen von einem notwendigen Investitionsvolumen von ca. 5 bis 20 Prozent p.a. des IT-Budgets von Unternehmen aus. Cyber Security ist jedoch kein Begeisterungsthema und es besteht die Gefahr, dass die ggf. knappen finanziellen Kapazitäten einseitig in die notwendige digitale Transformation von Produkten, Dienstleistungen und Geschäftsmodellen investiert werden. Begleitende Investitionen in IT-Sicherheit sind jedoch überlebensnotwendig. Zudem sollten Unternehmen die Sinnhaftigkeit von Versicherungen gegen die Folgen von Cyber-Attacken prüfen: Hier gibt es mittlerweile kostenseitig attraktive und viele, wenn auch nicht alle Folgen einer solchen Attacke abdeckende Angebote seitens der Versicherungswirtschaft.



Glossar

BKA	Bundeskriminalamt; dem Bundesministerium des Innern, für Bau und Heimat, nachgeordnete Bundesbehörden und eine der drei Polizeien des Bundes
Botnet	Ein Botnet oder Botnetz ist eine Gruppe automatisierter Schadprogramme oder Bots. Die Bots laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen.
BSI	Das Bundesamt für Sicherheit in der Informationstechnik ist eine in der Bundesstadt Bonn ansässige zivile obere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat, die für Fragen der IT-Sicherheit zuständig ist.
CDO	Der Chief Digital Officer ist in der Regel eine Position in der obersten Führungsebene von Unternehmen, die für die Planung und Steuerung der digitalen Transformation eines Unternehmens oder einer Organisation verantwortlich ist.
CEO Fraud	Der CEO Fraud ist eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden. Die Betrüger nehmen häufig die digitale Identität des CEO ein.
CIO	Der Chief Information Officer bzw. IT-Leiter nimmt allgemein in einem Unternehmen die Aufgaben der strategischen und operativen Führung der Informationstechnik wahr.
CISO	Ein Chief Information Security Officer bezeichnet die Rolle des Gesamtverantwortlichen für Informationssicherheit in einer Organisation.
COBIT	COBIT ist ein international anerkanntes Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives. COBIT definiert hierbei nicht vorrangig, wie die Anforderungen umzusetzen sind, sondern primär, was umzusetzen ist.
COSO	Das COSO ist eine freiwillige privatwirtschaftliche Organisation in den USA, die helfen soll, Finanzberichterstattungen durch ethisches Handeln, wirksame interne Kontrollen und gute Unternehmensführung qualitativ zu verbessern.
Digitale Erpressung	Cyberkriminelle nutzen Schadsoftware – sogenannte Ransomware – als Mittel der digitalen Erpressung. Daten auf infizierten Computern werden verschlüsselt, zur Wiederfreigabe soll ein Lösegeld bezahlt werden.
Hacker	Synonym für eine in IT-kundige Person, die illegal in fremde Computersysteme eindringt.
Hacktivismus/Hacktivist	Hacktivismus (Kofferwort aus Hack und Aktivismus, englisch hacktivism) ist als eine Variation des Cyberaktivismus die Verwendung von Computern und Computernetzwerken als Protestmittel, um politische und ideologische Ziele zu erreichen.
ISMS	Ein Information Security Management System ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

LKA	Ein Landeskriminalamt ist eine Einrichtung deutscher Landespolizeien, die in jedem der 16 Länder vorhanden ist. Üblicherweise handelt es sich um eine Landesoberbehörde – teilweise sind es unselbstständige Behördenteile.
Ransomware	Ransomware, auch Erpressungstrojaner, Erpressungssoftware, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann.
Red Teaming	Als Red Team oder Rotes Team wird eine unabhängige Gruppe bezeichnet, welche eine Organisation zur Verbesserung der Effektivität bringen soll, indem sie als Gegner auftritt. Ziel ist es dabei immer, Sicherheitslücken aufzuspüren, bevor ein externer Dritter diese ausnutzen kann.
Schadsoftware	Als Schadprogramm, Schadsoftware oder Malware – englisch badware, evilware, junkware oder malware – bezeichnet man Computerprogramme, die entwickelt wurden, um unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist damit ein Oberbegriff, der u.a. Computerviren umfasst.
Social Engineering	Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.
War Gaming	Beim Hacking ist ein War Game (oder Kriegsspiel) eine Herausforderung an die Cybersicherheit und ein Denksport, bei dem die Teilnehmer eine Schwachstelle in einem System oder einer Anwendung ausnutzen oder verteidigen oder Zugang zu einem Computersystem erlangen oder verhindern müssen.

Ihre Ansprechpartner

Lutz Meyer
Partner
Leiter Deloitte Private
Tel: +49 (0)211 8772 3502
lmeyer@deloitte.de

Markus Seiz
Director
Deloitte Private
Tel: +49 (0)711 16554 7699
mseiz@deloitte.de

Deloitte.
Private

Stand 06/2020