KPMG

e-Crime in der deutschen Wirtschaft 2019

Computerkriminalität im Blick

„Die Bedrohung durch Cyber-Kriminalität entwickelt sich ständig weiter und ist nicht nur hinter verschlossenen Türen von Unternehmen deutlich spürbar. Sie hat einen großen Einfluss auf Unternehmen, aber auch auf die tagtägliche Welt, wie beispielsweise Angriffe auf Versorgungsunternehmen oder auch die mögliche Beeinflussung von Wahlergebnissen zeigen. Die Professionalisierung ganzheitlicher Schutz- und Reaktionsmaßnahmen ist ein wichtiger Schritt, um dieser einer ‚Evolution' gleichkommenden Entwicklung der digitalen Bedrohungslage zu begegnen."

Michael Sauermann
Partner, Leiter Forensic Technology
Deutschland

Vorwort

Liebe Leserinnen und Leser,

mit dieser Studie beleuchtet KPMG zum nunmehr fünften Mal seit 2010 das Thema e-Crime in der deutschen Wirtschaft. Die Relevanz des Phänomens e-Crime ist nach wie vor enorm. Es vergeht nahezu kein Tag, an dem in der Presse nichts über Cyber-Angriffe zu lesen ist. Dabei stechen insbesondere zwei Aspekte heraus:

Einerseits kann Computerkriminalität jeden treffen. Nicht nur Branchenriesen, sondern auch Mittelständler aus der Kleinstadt stellen ein lukratives Angriffsziel für Kriminelle dar. Das unterstreicht die mediale Berichterstattung der vergangenen Monate.

Andererseits resultieren komplexe Systemlandschaften und neuartige Angriffsmuster in einer sehr breiten Angriffsfläche sowie einem hohen Maß an Anonymität, in dem potenzielle Täter agieren können. Oftmals kann bei externen Tätern nur vermutet werden, wer letztendlich für einen Cyber-Angriff verantwortlich ist. Hinzu kommt, dass digitale Spuren und die mediale Berichterstattung auf professionelle, staatliche Hacker-Gruppen hinweisen und diese bei der Begehung von e-Crime eine zunehmende Rolle spielen.

Diese Anonymität ist mitursächlich dafür, dass in der Computerkriminalität ein großes Dunkelfeld besteht. Unsere Studienergebnisse bestätigen dieses Bild, da sie zeigen, dass Betroffenen die Identifikation von Tätern größte Schwierigkeiten bereitet, was vermuten lässt, dass einzelne kriminelle Handlungen überhaupt nicht entdeckt werden.

Erschwerend kommt hinzu, dass sich die Methoden Cyber-Krimineller stetig weiterentwickeln. Nach wie vor erfreut sich dabei insbesondere Ransomware großer Beliebtheit. Derartige Angriffe sind zwar nicht neu, gleichwohl stellen wir geradezu eine „Evolution" dieser Schadsoftware fest, die immer effektiver wird, was sich in der Vielzahl medial wirksamer Vorfälle des vergangenen Jahres widerspiegelt – bei gleichzeitig hohem Schadenausmaß. Daher haben wir diese Thematik in dieser Studie genauer beleuchtet.

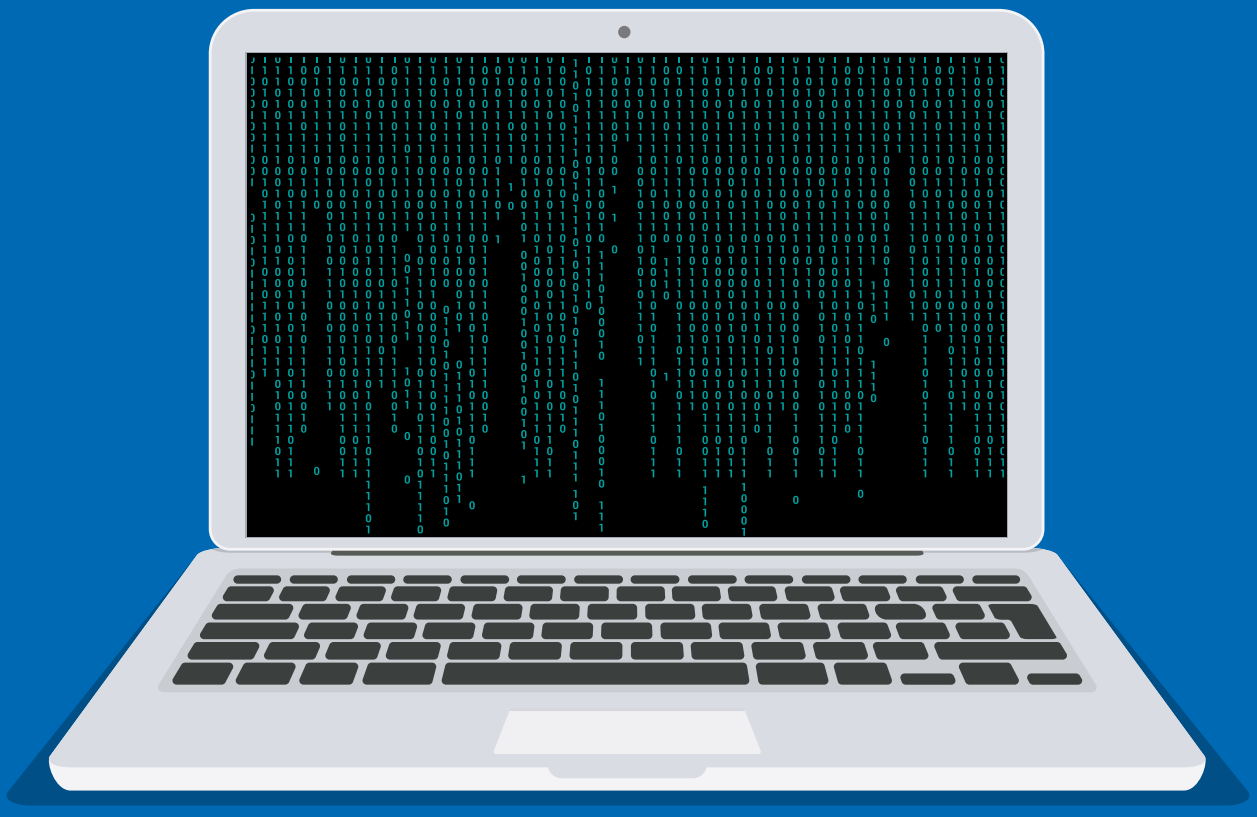
Um mit der Entwicklung der Täter Schritt zu halten, müssen sich Unternehmen immer wieder neu mit Maßnahmen zur Prävention, Aufdeckung und Aufklärung von sowie zur Reaktion auf e-Crime wappnen. Die Professionalisierung des Schutzes der IT-Infrastruktur sowie der unternehmenseigenen Datenbestände ist ein wichtiger Schritt, um diesen Wettlauf zu gewinnen. Beispiele derart professionalisierter Strukturen sind Unternehmenseinheiten wie Security Operations Center (SOC) und Computer Emergency Response Teams (CERT), denen wir einen eigenen Abschnitt in dieser Studie widmen.

Neben derartigen Maßnahmen nutzen immer mehr Unternehmen die Möglichkeit, sich mit einer Cyber-Versicherung zusätzlich abzusichern. Falls ein Vorfall nicht abgewendet werden kann, können die entstehenden Schäden damit zumindest teilweise gedeckt werden. Wie schon in der Studie des Jahres 2017 nehmen wir diesen Aspekt genauer unter die Lupe.

Ich wünsche Ihnen eine spannende und erkenntnisreiche Lektüre.

Michael Sauermann
Partner Compliance & Forensic
Leiter Forensic Technology Deutschland
KPMG AG Wirtschaftsprüfungsgesellschaft

Inhalt



Zahlen und Fakten

01 Wesentliche Ergebnisse der Studie

Von e-Crime sind nach wie vor viele Unternehmen betroffen, wobei zudem zu berücksichtigen ist, dass es ein erhebliches Dunkelfeld geben dürfte. Die Befragten sehen zunehmend Risiken für das eigene Unternehmen, doch verorten viele die Gefahr, tatsächlich betroffen zu sein, weiterhin eher bei Dritten als bei sich selbst.

- ✓ Die Befragten nehmen für die deutsche Wirtschaft im Allgemeinen ein deutlich höheres e-Crime-Risiko als für das eigene Unternehmen wahr (92 gegenüber 52 Prozent hohes/sehr hohes Risiko).
- ✓ Etwa zwei von fünf Unternehmen in Deutschland (39 Prozent) geben an, dass sie in den vergangenen zwei Jahren von e-Crime betroffen waren.
- ✓ Insbesondere die Identifikation der Täter bereitet große Schwierigkeiten. Fünf von sechs Betroffenen können sie lediglich der Kategorie „unbekannt extern" zuordnen. Hiermit geht auch die Gefahr einher, dass nicht nur Täter, sondern sogar Delikte gänzlich unerkannt bleiben.

Selbst im hochgradig technologiegeprägten Feld der Computerkriminalität sind menschliche Faktoren von entscheidender Bedeutung für deren Entstehung.

- ✓ Unachtsamkeit (90 Prozent) und unzureichend geschulte Mitarbeiter (83 Prozent) zählen zu den meistgenannten Faktoren, die e-Crime begünstigen. Eine angemessene Schulung und Sensibilisierung der Mitarbeiter kann also gar nicht hoch genug bewertet werden.
- ✓ Fünf von sechs Befragten nennen zudem eine mangelnde Sicherheitskultur, verbunden mit einem unzureichenden Risikoverständnis. Unternehmenskulturelle Aspekte – etwa der „Tone from the Top" – sind daher bei der Bekämpfung von e-Crime ebenfalls einzubeziehen.
- ✓ Neben menschlichen und kulturellen Aspekten ist der Faktor Technologie nicht zu vernachlässigen. Die zunehmende Komplexität der eingesetzten Technologie stellt die Befragten (83 Prozent) vor große Herausforderungen und vielen fällt es daher zunehmend schwer, erste Anzeichen von Verdachtsfällen zu erkennen (85 Prozent).

Der Stellenwert vorbeugender Maßnahmen nimmt im Vergleich zur vorigen Studie wieder zu. Eine Mehrheit der getätigten Investitionen entfällt auf den Bereich Prävention, doch insgesamt ist die Investitionsbereitschaft nach wie vor gering.

- ✓ Im Vergleich zur Studie des Jahres 2017 werden die meisten der abgefragten Präventionsmaßnahmen wieder häufiger umgesetzt. Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeiter (88 Prozent), die Verschlüsselung von Daten und Datenträgern (87 Prozent) sowie die regelmäßige Identifizierung des Schutzbedarfs von Daten und Systemen (79 Prozent) sind die meistgenannten präventiven Maßnahmen.
- ✓ Knapp zwei Drittel der Befragten (65 Prozent) sehen entweder Schwierigkeiten bei der internen Rekrutierung und Weiterbildung der Beschäftigten oder finden kaum geeignete externe Bewerber.
- ✓ Nach wie vor fallen die Investitionsvolumina für die Bekämpfung von e-Crime relativ gering aus. Lediglich knapp ein Viertel der Befragten investiert mehr als 50.000 Euro, wobei durchschnittlich die Hälfte (50,3 Prozent) der Investitionen auf die Prävention von Computerkriminalität entfällt.

Beim Schutz von IT-Infrastruktur und Unternehmensdaten spielen sogenannte Security Operations Center (SOC) und Computer Emergency Response Teams (CERT) eine immer wichtigere Rolle, da sie merklich zur e-Crime-Bekämpfung beitragen können.

- ✓ Jeweils rund ein Fünftel der Befragten verfügt über ein SOC oder CERT (22 beziehungsweise 21 Prozent) mit durchschnittlich jeweils sieben Mitarbeitern. 12 Prozent der Befragten betreiben beide Einheiten.
- ✓ In SOC und CERT sind in der Regel mehrere unterschiedliche Aufgabenbereiche vereint. So liegen bei etwa drei von vier Unternehmen Echtzeitanalysen der Systeme beziehungsweise des Systemzustands, die Vorfallsbehandlung, die physische Sicherheit, Bedrohungsanalysen und Sensibilisierungsmaßnahmen im Verantwortungsbereich dieser Einheiten.
- ✓ Gut ein Drittel der Befragten (35 Prozent) bewertet die Wirksamkeit des eigenen SOC oder CERT als sehr gut, weitere 61 Prozent immerhin als eher gut. Gleichwohl konstatieren etwa drei Viertel der Befragten Versäumnisse im Hinblick auf diese Einheiten, zumeist eine unzureichende personelle Ausstattung (37 Prozent).

Der Markt für Cyber-Versicherungen wächst. Unternehmen wissen zunehmend um die Möglichkeit, eine solche Versicherung abzuschließen, und immer mehr haben dies in den vergangenen drei Jahren getan.

- ✓ Zwei Dritteln der Befragten (66 Prozent) sind Cyber-Versicherungen bekannt (2017: 55 Prozent). Mehr als ein Viertel dieser Unternehmen (27 Prozent) verfügt über eine solche Police, weitere 28 Prozent erwägen den Abschluss.
- ✓ Cyber-Versicherungen sind zunehmend gefragt, doch der Markt ist noch jung. Zwei Drittel der Policen (66 Prozent) wurden in den vergangenen drei Jahren abgeschlossen. Das „Durchschnittsalter" der Versicherungen beträgt 2,9 Jahre. Bei umsatzstarken Unternehmen und Finanzdienstleistern haben sie im Durchschnitt allerdings schon mehr als fünf Jahre Bestand.
- ✓ Gut die Hälfte der Befragten (55 Prozent) möchte keine Versicherung abschließen und begründet dies in der geringen eigenen Betroffenheit. Gleichwohl teilt diese Meinung dennoch auch knapp jedes zweite der tatsächlich bereits betroffenen Unternehmen (47 Prozent).

Das Phänomen Ransomware ist den Unternehmen mittlerweile ein Begriff. Allerdings können Angriffe große Schäden bei Unternehmen verursachen, die nicht über angemessene Schutzvorkehrungen verfügen.

- ✓ Nach den großen Ransomware-Fällen der vergangenen Jahre wie WannaCry, NotPetya und Emotet in Verbindung mit Ryuk, sind inzwischen fast alle Befragten mit dieser Art von e-Crime vertraut (2017: 49 Prozent nicht mit Thema vertraut).
- ✓ Knapp ein Drittel der Befragten war in den vergangenen zwei Jahren Opfer eines Ransomware-Angriffs (31 Prozent), weitere 28 Prozent konnten Versuche abwehren.
- ✓ Bei mehr als einem Viertel der Betroffenen kam es infolge der Attacke zu einem Betriebsausfall, der gravierende Konsequenzen haben kann. So waren bei jedem fünften Unternehmen mehr als 75 Prozent der IT-Landschaft betroffen und bei etwa einem Fünftel (22 Prozent) dieser Unternehmen dauerte es sogar mehr als zwei Tage, bis der Betrieb wieder aufgenommen werden konnte.

Definition e-Crime

e-Crime – im Rahmen dieser Studie gleichbedeutend mit den Begriffen Computerkriminalität und Cyber-Kriminalität – bezeichnet die Ausführung wirtschaftskrimineller Handlungen unter Einsatz von Informations- und Kommunikationstechnologien zum Schaden einer Einzelperson, eines Unternehmens oder einer Behörde. Diese Form der Kriminalität kann sowohl zur Schädigung von Sachwerten, zum Beispiel durch Sabotage an Computersystemen, als auch zur Verletzung von Verfügungsrechten an immateriellen Gütern, etwa durch Diebstahl von Quellcodes, von Kundendaten oder von anderen Informationen, führen. Infolge solcher Schäden können zudem die Geschäftsprozesse eines Unternehmens empfindlich beeinträchtigt werden. Informations- und Kommunikationssysteme können hierbei Ziel der Tathandlung, aber auch Tatwerkzeug an sich sein. e-Crime bezeichnet somit nicht nur Angriffe von außen, die mithilfe von Schadsoftware und unter Ausnutzung von Systemlücken über das Internet erfolgen („Cybercrime"), sondern umfasst auch das breite Spektrum anderer Straftaten, die Informations- und Kommunikationstechnologie als Werkzeug einsetzen.

Eine weitere e-Crime-Komponente sind „klassische" wirtschaftskriminelle Handlungen, die durch den Einsatz von Informations- und Kommunikationstechnologie erst ermöglicht oder zumindest erleichtert werden oder bei denen IT-Werkzeuge der Verschleierung dienen. Ein Beispiel hierfür ist der sogenannte Fake-President-Betrug, auch CEO Fraud genannt. Dabei geben sich Kriminelle – zum Teil unter Zuhilfenahme zuvor gestohlener oder abgehörter Informationen – als Führungskräfte oder externe Berater aus und verleiten Mitarbeiter mit gefälschten E-Mails dazu, Zahlungen auf von ihnen kontrollierte Konten zu tätigen.

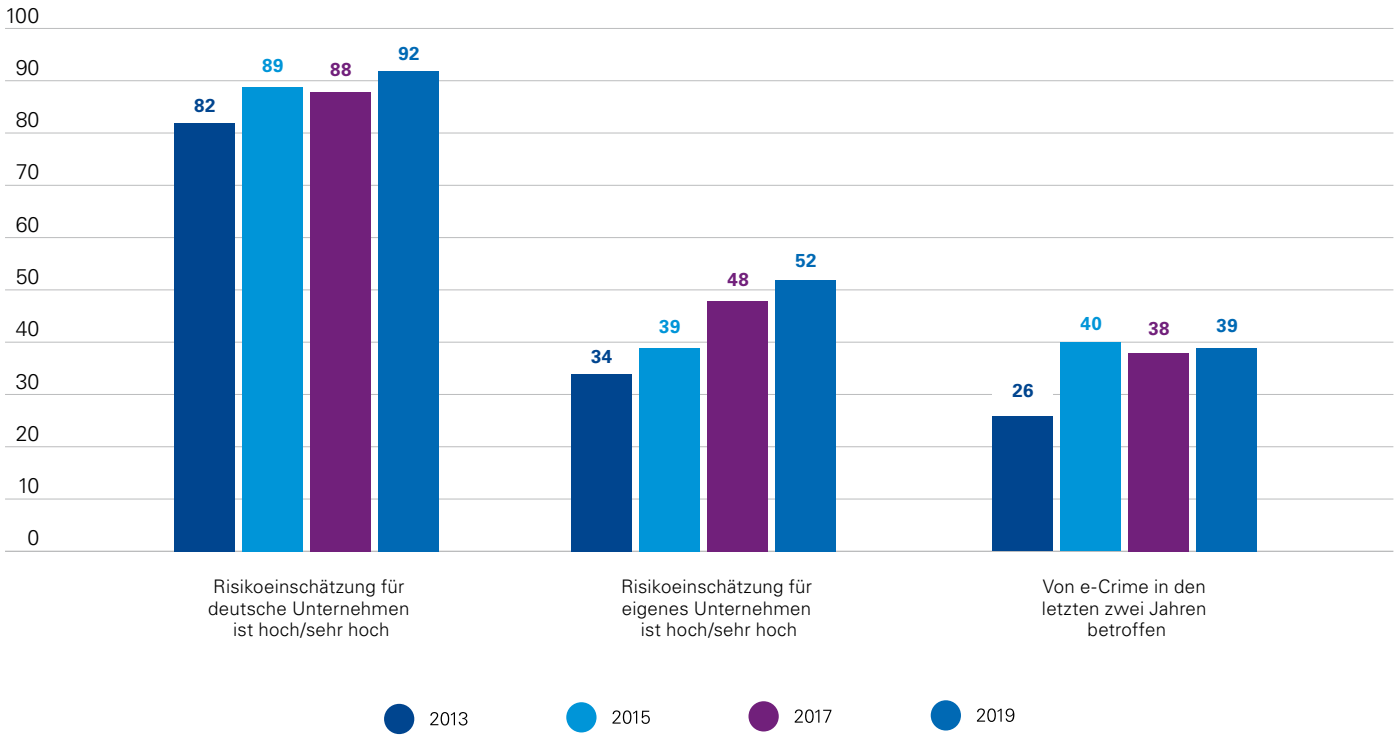
e-Crime im Profil

02 Risikoprofil und Kosten

2.1. Risikowahrnehmung und Betroffenheit

Computerkriminalität stellt für Unternehmen weiterhin ein massives Risiko dar. Mehr als neun von zehn Befragten schätzen die Gefahr der Betroffenheit durch e-Crime für deutsche Unternehmen als hoch oder sehr hoch ein (Abb. 1). Explizit für sehr hoch hält dieses Risiko gut ein Viertel aller Befragten und sogar gut ein Drittel derjenigen, deren Unternehmen in den vergangenen zwei Jahren selbst betroffen war. Lediglich 22 Prozent der nicht betroffenen Studienteilnehmer nehmen ein sehr hohes Risiko wahr. Die Betroffenheit führt somit zu einer zusätzlichen Sensibilisierung für die Gefahrenlage.

Abb. 1: Vergleich Risikoeinschätzung und Betroffenheit
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Ein sehr hohes Risiko für das eigene Unternehmen sehen nur 7 Prozent der Studienteilnehmer, wohingegen dieser Wert für die Untergruppe der betroffenen Unternehmen bei 14 Prozent liegt. Insgesamt bezeichnen immerhin 68 Prozent der Betroffenen das Risiko von e-Crime als hoch oder sehr hoch. Lediglich 41 Prozent der nicht Betroffenen teilen diese Einschätzung.

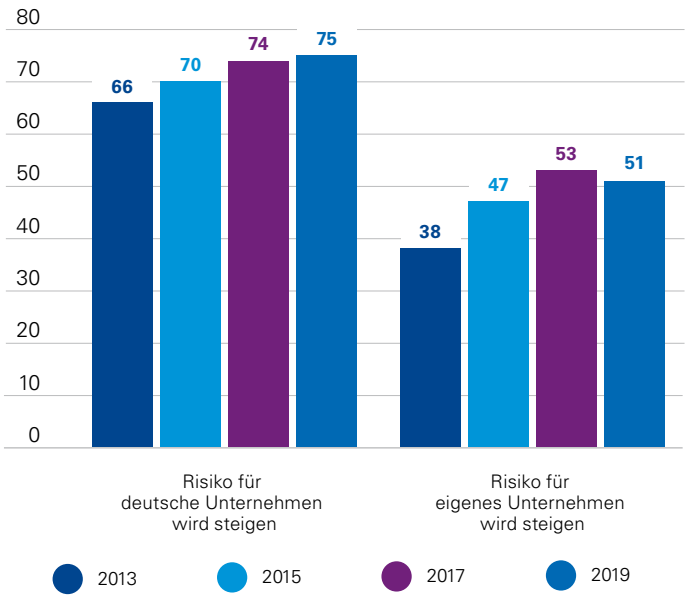
In der vorliegenden Publikation teilen wir die Unternehmen in die Kategorien groß, mittel und klein ein, basierend auf ihrem jeweiligen Umsatz. Unternehmen mit einem Umsatz von mehr als drei Milliarden Euro gelten als groß, solche mit einem Umsatz zwischen 250 Millionen und drei Milliarden Euro fallen unter „mittel" und bei einem Umsatz von weniger als 250 Millionen Euro gilt die Kategorie klein.

Zudem fällt auf, dass in kleinen Unternehmen die eigenen Risiken als deutlich geringer wahrgenommen werden als in größeren (47 Prozent hoch/sehr hoch gegenüber 57 beziehungsweise 58 Prozent hoch/sehr hoch). Da allerdings bei der Frage, für wie drängend die Risiken generell gehalten werden, keine signifikanten Unterschiede nach Unternehmensgrößen auszumachen sind, ist unklar, ob die Entscheider kleiner Unternehmen die eigene Gefahrenlage unterschätzen.

Eine mögliche Ursache für diese Wahrnehmung könnte in der tatsächlich festgestellten Betroffenheit liegen. Insgesamt waren in den vergangenen zwei Jahren knapp zwei von fünf deutschen Unternehmen von e-Crime betroffen, wobei kleine Unternehmen (35 Prozent) prozentual seltener betroffen waren als mittlere (42 Prozent) und große (45 Prozent). Aus diesen Zahlen zu folgern, dass das Risiko eines e-Crime-Angriffs für kleinere Unternehmen geringer sei, ist allerdings trügerisch. Denn es gilt zu bedenken, dass die hohe Betroffenheit großer Unternehmen auch durch das sogenannte Kontrollparadoxon zu erklären sein kann. Dieser Begriff bezeichnet den Umstand, dass große Unternehmen aufgrund ihrer überdurchschnittlich guten Aufdeckungsmechanismen mit einer größeren Wahrscheinlichkeit als andere Unternehmen Delikte aufdecken – und somit zumindest auf dem Papier häufiger betroffen sind als andere. Kleinere Unternehmen laufen somit Gefahr, die Risiken von Computerkriminalität aufgrund einer „unzuverlässigen" Statistik zu unterschätzen. Zusätzliche Brisanz ergibt sich daraus, dass sie nicht über in gleicher Weise effektive Maßnahmen zur Verhinderung und Aufklärung von e-Crime verfügen wie große Unternehmen.

Zudem ist angesichts der Eigenheiten von Computerkriminalität – insbesondere immer komplexerer Systemlandschaften, immer neuer Angriffsmuster und eine daraus resultierende hohe Anonymität der Täter – davon auszugehen, dass es Unternehmen aller Größenordnungen oftmals nicht möglich sein wird, die tatsächliche Betroffenheit in Gänze abzubilden. Unterstrichen wird dies durch einen Blick auf die festgestellten Täter: Die absolute Mehrheit der Betroffenen (85 Prozent) kann sie nur der Kategorie „unbekannte Externe" zuordnen. Ein solch hoher Anteil nicht identifizierter Täter lässt vermuten, dass viele Taten gar nicht erst entdeckt werden und ein großes Dunkelfeld besteht. Von daher ist durchaus denkbar, dass die tatsächliche Betroffenheit höher liegt als von den Befragten angenommen.

Abb. 2: Risikoerwartung für die kommenden zwei Jahre
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Die Diskrepanz zwischen Eigen- und Fremdwahrnehmung zeigt sich auch bei der Risikoeinschätzung für die kommenden zwei Jahre: Drei Viertel der Befragten vermuten, dass das e-Crime-Risiko für deutsche Unternehmen in diesem Zeitraum steigen wird (Abb. 2).

Für das eigene Unternehmen rechnen 51 Prozent der Befragten mit einem steigenden Risiko, 44 Prozent erwarten keine Veränderung der Gefahrenlage. Betroffene zeigen auch bei dieser Frage eine höhere Sensibilisierung als nicht Betroffene (56 gegenüber 47 Prozent). Für die Unternehmen wird Computerkriminalität demnach auch in den kommenden zwei Jahren ein zentrales Thema sein.

Letztlich lässt sich sagen, dass sich diese Lücke trotz der weiterhin großen Diskrepanz zwischen der Risikowahrnehmung für das eigene Unternehmen und für die deutschen Unternehmen insgesamt seit einigen Jahren schließt. Dies zeugt von der Aufmerksamkeit der Unternehmen in Bezug auf Computerkriminalität. Sie realisieren zunehmend, dass es sich nicht um ein zwar medial häufig thematisiertes, aber doch abstraktes Phänomen handelt, sondern um eines, das auch das eigene Unternehmen tatsächlich jederzeit treffen kann.

2.2. Deliktsspezifische Risikowahrnehmung und Betroffenheit

Bei der Betrachtung der einzelnen abgefragten Delikte rücken Datendiebstahl und Computerbetrug im Vergleich zu den Ergebnissen voriger Studien verstärkt in den Fokus. Jeweils 88 Prozent der Befragten bezeichnen das Risiko derartiger Delikte als hoch oder sehr hoch, wovon knapp 30 Prozent auf die Kategorie „sehr hoch“ entfallen (Abb. 3). Bereits von e-Crime betroffene Unternehmen zeigen sich diesbezüglich nochmals sensibilisierter. Ein sehr hohes Risiko für Datendiebstahl sehen 32 Prozent der Betroffenen, für Computerbetrug 35 Prozent.

In der Studie abgefragte Delikte in Kürze[1]

Computerbetrug: betrügerische Handlungen unter Ausnutzung von Kommunikations- und Informationstechnologien und per Manipulation von Datenverarbeitungssystemen und -prozessen (zum Beispiel widerrechtliche Nutzung von Online-Banking-Funktionen)

Manipulation von Konto- und Finanzdaten: unberechtigte Veränderung von Konto- und Finanzdaten in Buchhaltungs- oder Zahlungssystemen

Datendiebstahl/Ausspähen oder Abfangen von Daten: unberechtigte Aneignung von Daten unter Überwindung einer Zugangssicherung oder auch unberechtigtes Aufzeichnen, Mithören oder Mitlesen von Daten, die nicht öffentlich übermittelt werden (etwa E-Mail-Versand, Instant Messaging, Netzwerkverkehr, IP-Telefonie), aber auch von „natürlichen“ Gesprächen über technische Hilfsmittel

Verletzung von Urheberrechten: Verstoß gegen die Verwertungs- und Schutzrechte urheberrechtlich geschützter elektronischer Daten (beispielsweise rechtswidriges Kopieren und Verwenden von Software oder Inhalten audiovisueller Medien)

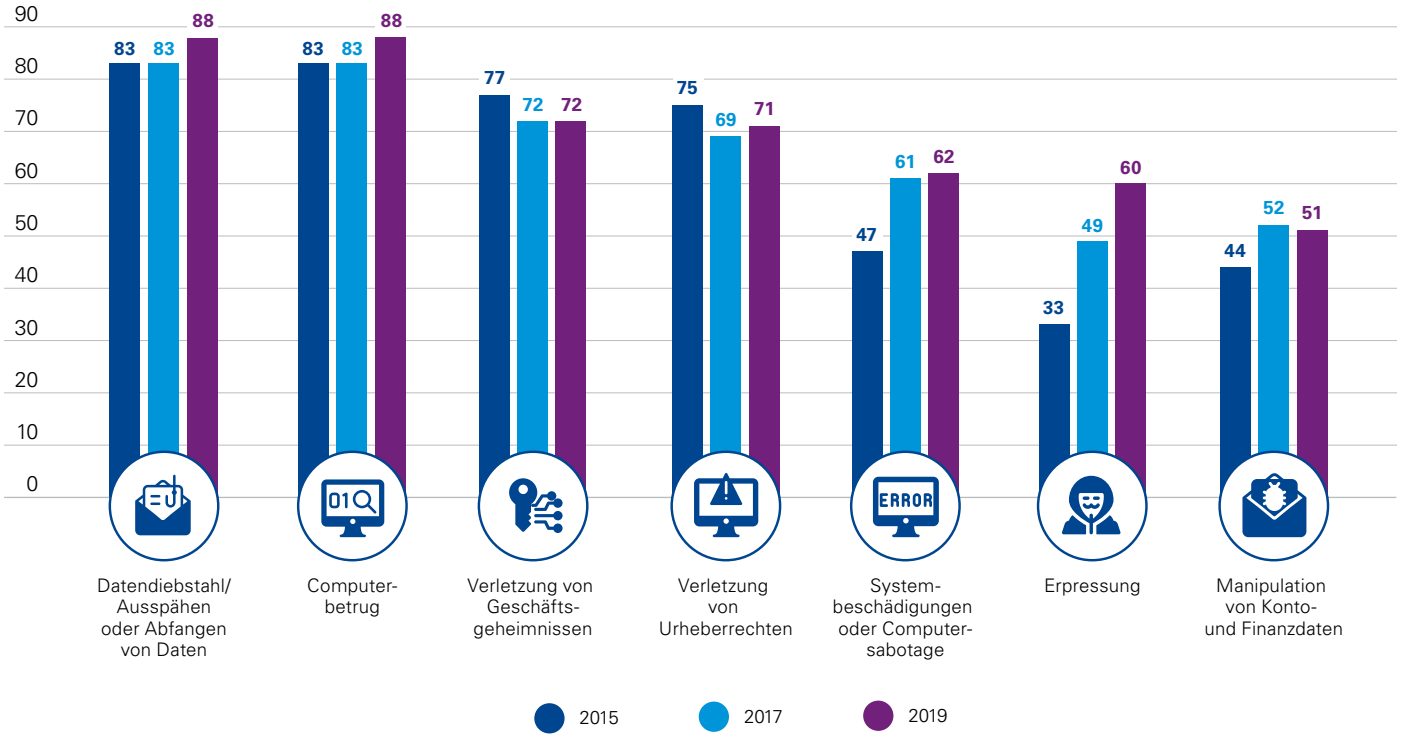
Verletzung von Geschäftsgeheimnissen: unbefugte Aneignung, Nutzung und Weitergabe vertraulicher, nicht allgemein zugänglicher und mit Geheimhaltungsmaßnahmen geschützter Informationen eines Unternehmensinhabers unter Nutzung von Kommunikations- und Informationstechnologien

Systembeschädigungen oder Computersabotage: Störung von Datenverarbeitungsprozessen durch Löschung, Veränderung oder das Unbrauchbarmachen von Daten, durch Eingabe oder Übermittlung von Daten in der Absicht, anderen einen Nachteil zuzufügen, oder durch Beschädigung, Manipulation oder Zerstörung von Computern, Netzwerken oder Datenträgern

Erpressung: Nötigung zu einem Handeln, Dulden oder Unterlassen unter Androhung von e-Crime-Handlungen zwecks Bereicherung am Vermögen des Genötigten

[1] Die Kurzdefinitionen sind an Straftatbestände angelehnt.

Abb. 3: Deliktsspezifische Risikowahrnehmung
Angaben in Prozent; Risikoeinschätzung hoch/sehr hoch

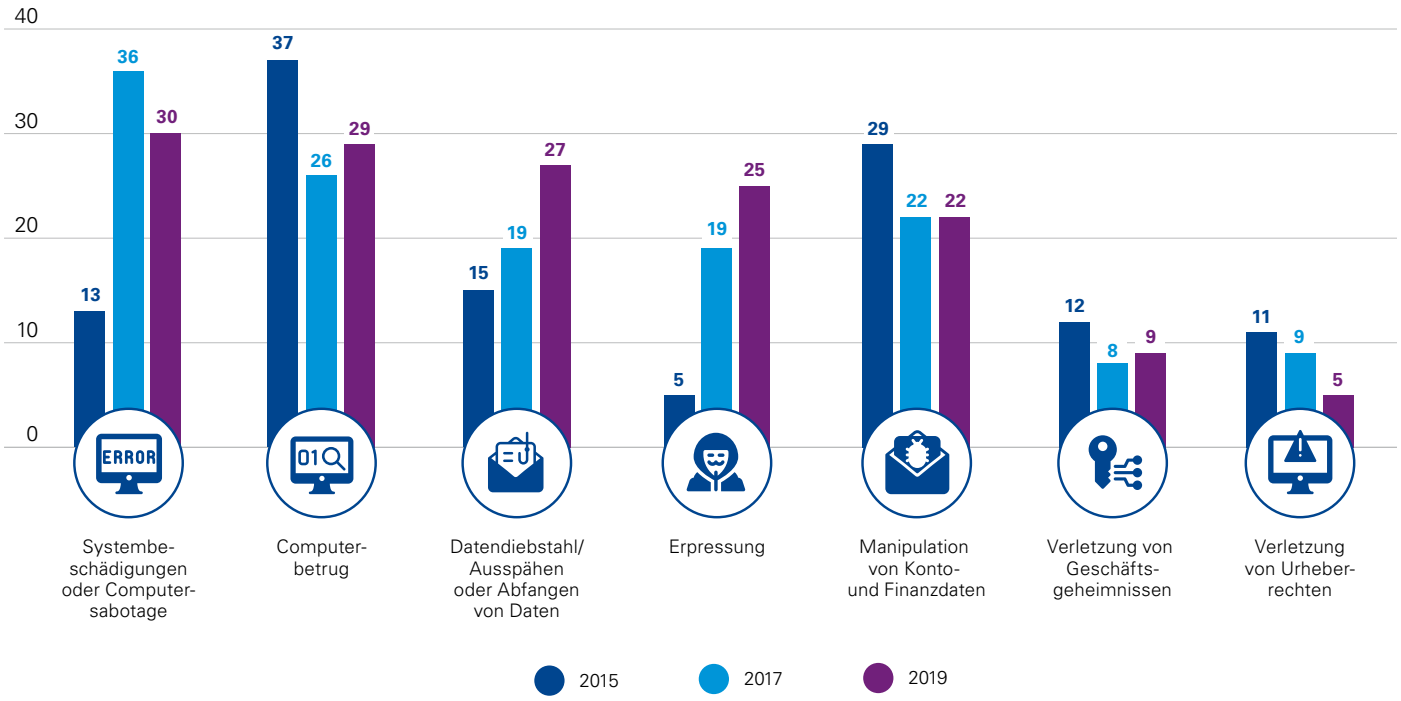


Quelle: KPMG in Deutschland, 2019

Zwar werden die Risiken einer Konfrontation mit Computerbetrug oder Datendiebstahl mit einigem Abstand als am höchsten bewertet, doch sind diese beiden Deliktsarten nicht die, die am häufigsten auftreten. Mit Betroffenheitswerten von 29 Prozent (Computerbetrug) und 27 Prozent (Datendiebstahl) liegen sie an zweiter und dritter Stelle (Abb. 4), wobei Finanzdienstleister besonders häufig von Computerbetrug betroffen waren (50 Prozent).

Mit Blick auf Datendiebstahl bedeutet die Betroffenheit von 27 Prozent einen Anstieg um 8 Prozentpunkte gegenüber der vorangegangenen Befragung. Somit nimmt die in den bisherigen Studien festgestellte Diskrepanz zwischen sehr hoher Risikowahrnehmung und geringer Betroffenheit zumindest etwas ab. Dennoch ist gerade daten- und technologiebezogenen Delikten die Gefahr inhärent, dass Täter in nahezu vollkommener Anonymität handeln können. Somit stellt die Entdeckung solcher Taten Unternehmen vor ungleich größere Herausforderungen als beispielsweise

Abb. 4: Betroffenheit
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

„klassische" analoge Delikte, wie sich am Beispiel Diebstahl deutlich zeigt: Anders als der Diebstahl physischer Güter bedeutet Datendiebstahl zumeist gerade nicht, dass Daten verschwunden sind, womit der reine Verlust nicht durch eine numerische Prüfung des Datenbestands festzustellen ist. Viel häufiger ist der Fall, dass die Täter Daten kopieren und sich auf diesem Weg unzählige Möglichkeiten erschließen. Es ist also bei computerkriminellen Handlungen von einer hohen Dunkelziffer auszugehen, sodass die Befragten ihre tatsächliche Betroffenheit möglicherweise nicht korrekt benennen können.

Bei Systembeschädigungen oder Computersabotage lässt sich ein gegenläufiges Phänomen feststellen. Einerseits handelt es sich hierbei um das Delikt mit der höchsten Betroffenheitsrate (30 Prozent), andererseits fällt die Risikowahrnehmung der Befragten mit lediglich 62 Prozent (hohes und sehr hohes Risiko) vergleichsweise gering aus. Ähnliches lässt sich über die Manipulation von Konto- und Finanzdaten sagen (Betroffenheit: 22 Prozent, Risikowahrnehmung: 52 Prozent hoch/sehr hoch).

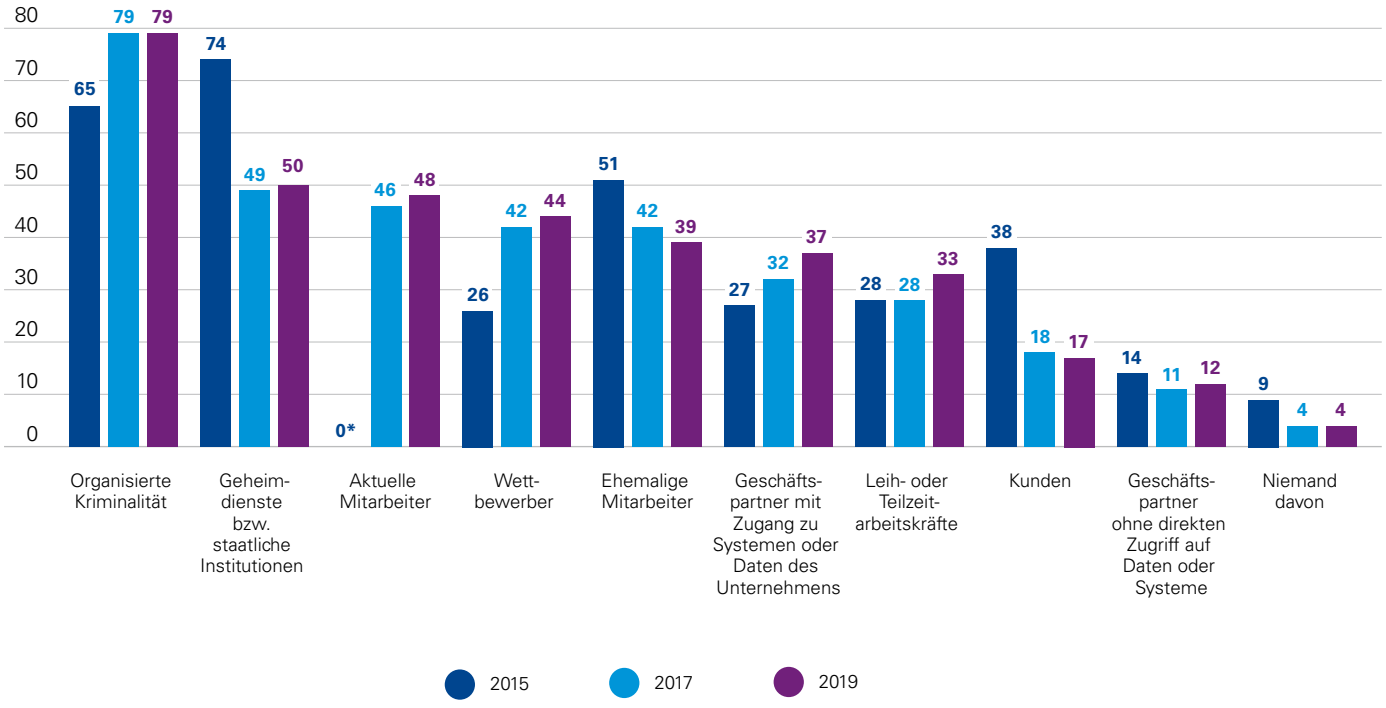
Gegenbeispiele sind nach wie vor die Verletzung von Geschäftsgeheimnissen wie auch die von Urheberrechten. Liegt die Betroffenheit hier bei lediglich 9 beziehungsweise 5 Prozent, bezeichnen gleichwohl gut 70 Prozent der Umfrageteilnehmer das Risiko der Betroffenheit durch diese Deliktsarten als hoch oder sehr hoch.

Mit Blick auf Erpressungsdelikte zeigt die jüngste Befragung – wie auch die vorhergehende – die größte Weiterentwicklung. So steigt die Betroffenheit von 19 auf 25 Prozent und die Risikowahrnehmung von 49 auf 60 Prozent. Es ist davon auszugehen, dass dieser Trend insbesondere durch große Ransomware-Fälle, wie es sie in der Vergangenheit beispielsweise mit WannaCry oder NotPetya gab, weiterhin befeuert wird. Schließlich geht keiner dieser Vorfälle ohne Erpressung einher.[2] Da das Phänomen Ransomware ungebrochen relevant ist, ist davon auszugehen, dass auch die Deliktsart der Erpressung mittels e-Crime weiter im Blickpunkt der Befragten bleiben wird.

2.3. Personengruppen und Länder in Verbindung mit e-Crime und tatsächliche Täter

Vier von fünf Befragten sehen die Organisierte Kriminalität als besonders bedeutsame Gefahrenquelle für ihr Unternehmen (79 Prozent). Schon in der Befragung des Jahres 2017 handelte es sich hierbei um die meistgenannte Tätergruppe. Aufgrund immer wieder neuer Angriffsmuster und vielfach auch aufgrund des Mangels an entsprechenden Gegenmaßnahmen bietet Computerkriminalität ein hohes Schadenspotenzial und ist daher für professionell organisierte Gruppen besonders attraktiv (Abb. 5). Allerdings ist zu beachten, dass es zur Begehung von Computerkriminalität derart organisierter Strukturen nicht unbedingt bedarf – das Gefahrenpotenzial von Einzeltätern zeigte nicht zuletzt der Hacking-Angriff auf den Deutschen Bundestag Ende 2018. Zu berücksichtigen ist in diesem Kontext auch die immer stärkere Verbreitung von „Hacking as a Service“, mit dem auch technisch nicht versierte Personen per „Dienstleistung“ zum e-Crime-Täter werden können.

Abb. 5: Potenziell gefährliche Personengruppen
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

* Wurde 2015 nicht abgefragt.

[2] Bei NotPetya handelt es sich um einen sogenannten Wiper. Getarnt als Erpressungstrojaner, bot die Software keine Möglichkeit, die verschlüsselten Daten zu entschlüsseln, sondern war ausschließlich destruktiv.

Geheimdienste und andere staatliche Institutionen werden von mehr als der Hälfte der Studienteilnehmer als möglicher Urheber computerkrimineller Delikte gesehen. Derartige Akteure haben sich infolge der Veröffentlichungen durch den Whistleblower Edward Snowden als am zweitmeisten genannte Personengruppe „etabliert". Angesichts der steten medialen Präsenz staatlichen Handelns im Zusammenhang mit Computerkriminalität ist davon auszugehen, dass die Berichterstattung einen nicht unbedeutenden Einfluss auf die Wahrnehmung der Unternehmen hat. Schließlich kam bei den meisten der großen Hacking-Angriffe der vergangenen zwei Jahre immer wieder die Frage auf, ob staatlich finanzierte Gruppen aus Russland, China oder auch Nordkorea dafür verantwortlich sind. In der Praxis ist es wiederum kaum vorstellbar, dass tatsächlich die Hälfte der Befragten kriminellen Handlungen staatlicher Akteure ausgesetzt sein sollte beziehungsweise sie diese überhaupt als Täter feststellen könnten. Vermutlich ist die Furcht vor staatlichen Akteuren unverhältnismäßig, möglicherweise verzerrt durch die mediale Präsenz.

Aktuelle Mitarbeiter werden ebenfalls von knapp der Hälfte der Befragten als Gefahrenquelle für das eigene Unternehmen eingestuft (48 Prozent) – ehemalige Mitarbeiter hingegen spielen eine weniger gravierende Rolle (39 Prozent, wobei diese Zahl über die Jahre stetig abnimmt). Ins Auge fällt hier zudem, dass große Unternehmen aktuelle Mitarbeiter häufiger als mittlere und kleine Unternehmen für einen Risikofaktor halten (61 Prozent).

Grundsätzlich zeigt sich die Tendenz, mit zunehmendem Umsatz alle Personengruppen auch zunehmend als Gefahrenquelle für e-Crime zu bewerten. Unter anderem werden von den „Großen" Geschäftspartner mit Zugang zu Unternehmenssystemen oder -daten (48 Prozent; allgemein: 37 Prozent) sowie Leih- oder Teilzeitarbeitskräfte (46 Prozent; allgemein: 33 Prozent) besonders kritisch gesehen.

Die Ursache hierfür dürfte schlicht die Größe der Unternehmen sein: Die höheren Zahl an Mitarbeitern und Geschäftspartnern führt zu unübersichtlicheren und somit schwerer zu schützenden Strukturen, sodass grundsätzlich eine erhöhte Anfälligkeit gegenüber kriminellen Handlungen unterschiedlicher Personengruppen besteht.

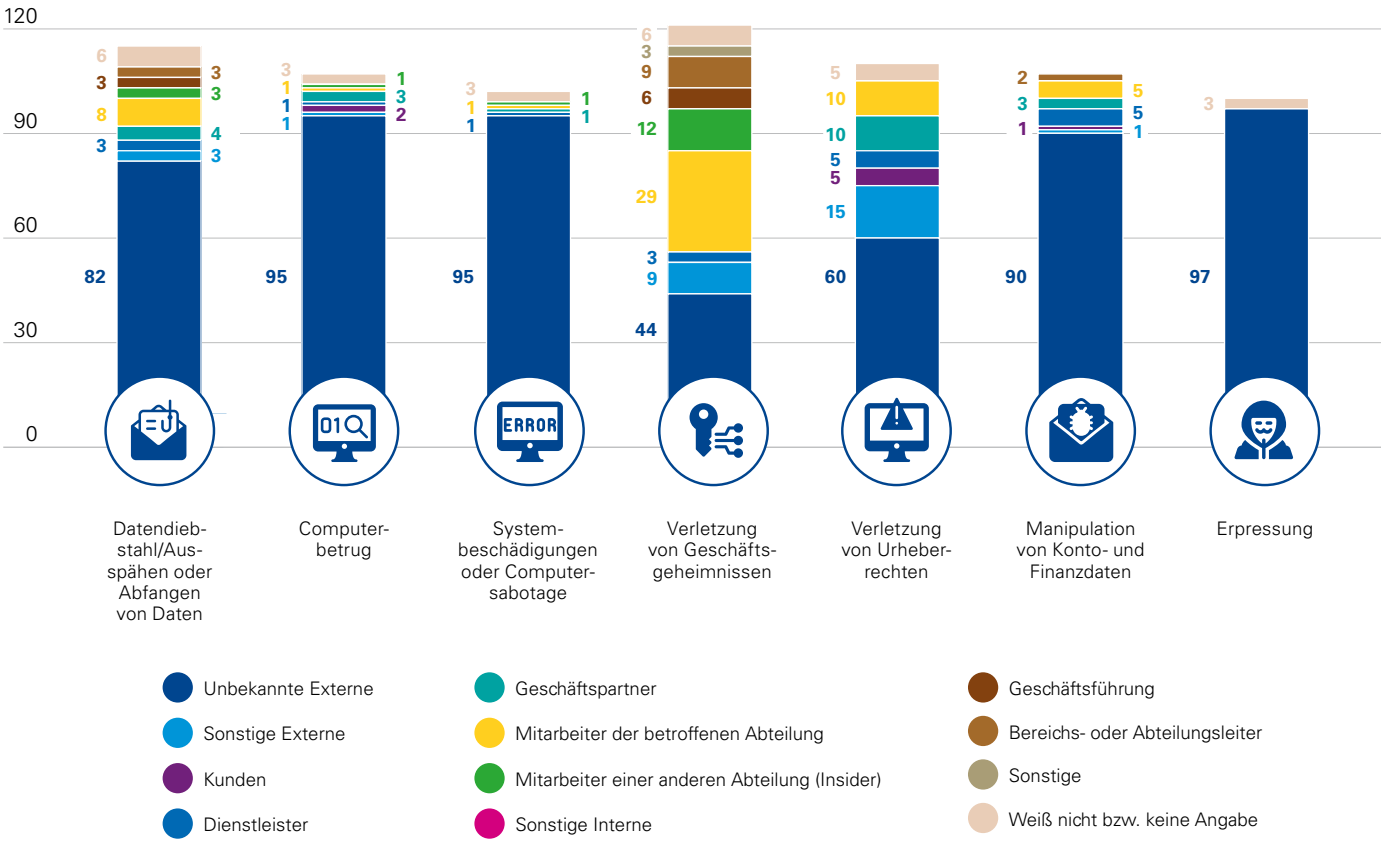
Der Risikofaktor Geschäftspartner mit Systemzugang gewinnt im Übrigen in der Einschätzung aller Befragten weiterhin an Bedeutung (2015: 27 Prozent; 2017: 32 Prozent; 2019: 37 Prozent). Umso wichtiger ist die sorgfältige Auswahl solcher Partner. Wer deren Integrität durch entsprechende Maßnahmen wie Due Diligences sicherstellen kann, mindert das e-Crime-Risiko beträchtlich.

Immerhin 44 Prozent der Studienteilnehmer sehen Wettbewerber als eine bedeutsame Gefahrenquelle, in der Industrie gilt dies sogar für die Hälfte der Befragten. Insbesondere im Hinblick auf Sabotagedelikte oder die Verletzung von Geschäftsgeheimnissen dürfte diese Personengruppe von Belang sein.

Der Blick auf die tatsächlichen Täter lässt nur wenige Rückschlüsse darauf zu, inwieweit die Angaben zu potenziell gefährlichen Personengruppen die Realität abbilden, da der überwiegende Anteil der Befragten (85 Prozent) die Täter der Kategorie „unbekannte Externe" zuordnet. Zum Vergleich: Am zweithäufigsten – mit nur 4 Prozent – werden Mitarbeiter der jeweils betroffenen Abteilung genannt. Hier zeigen sich das zuvor schon skizzierte Dunkelfeld und die enormen Herausforderungen, vor denen Unternehmen bei der e-Crime-Aufdeckung stehen.

Für die Gesamtheit aller Delikte machen Unternehmensexterne 91 Prozent der von den Betroffenen benannten Täter aus. Lediglich bei der Verletzung von Geschäftsgeheimnissen sind Interne als Täter von hoher Relevanz (Abb. 6).

Abb. 6: Täterherkunft[3]
Angaben in Prozent

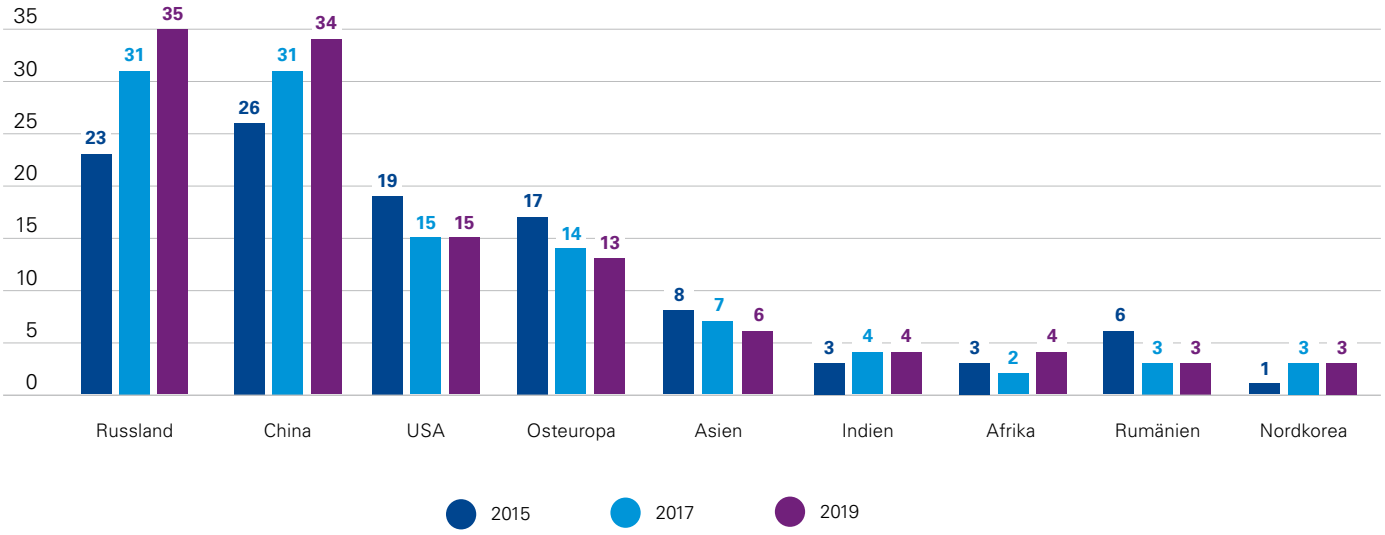


Quelle: KPMG in Deutschland, 2019

[3] Da auch ein potenzielles Zusammenwirken interner und externer Täter abgefragt wurde („kollusives Handeln"), sind Werte über 100 Prozent möglich.

Wie bereits bei den vorangegangenen Umfragen sieht etwas mehr als die Hälfte der Befragten (52 Prozent) einen Zusammenhang zwischen bestimmten Ländern oder Regionen und e-Crime, wobei sich die prozentuale Verteilung gegenüber der Studie des Jahres 2017 nur geringfügig verändert hat (Abb. 7). Weiterhin werden Russland und China bei dieser Frage am häufigsten genannt (35 beziehungsweise 34 Prozent). Die Befragten betrachten beide Länder somit etwas argwöhnischer als 2017 (jeweils 31 Prozent), was an der medialen Präsenz dieser Länder liegen könnte, beispielsweise in Form von Berichten über staatlich gesteuerte Angriffe. Die weltweit angespannte politische Lage könnte ebenfalls ihren Teil zu dieser Einschätzung beitragen.

Abb. 7: Risikobehaftete Länder und Regionen
Abbildung der meistgenannten Länder und Regionen, Angaben in Prozent



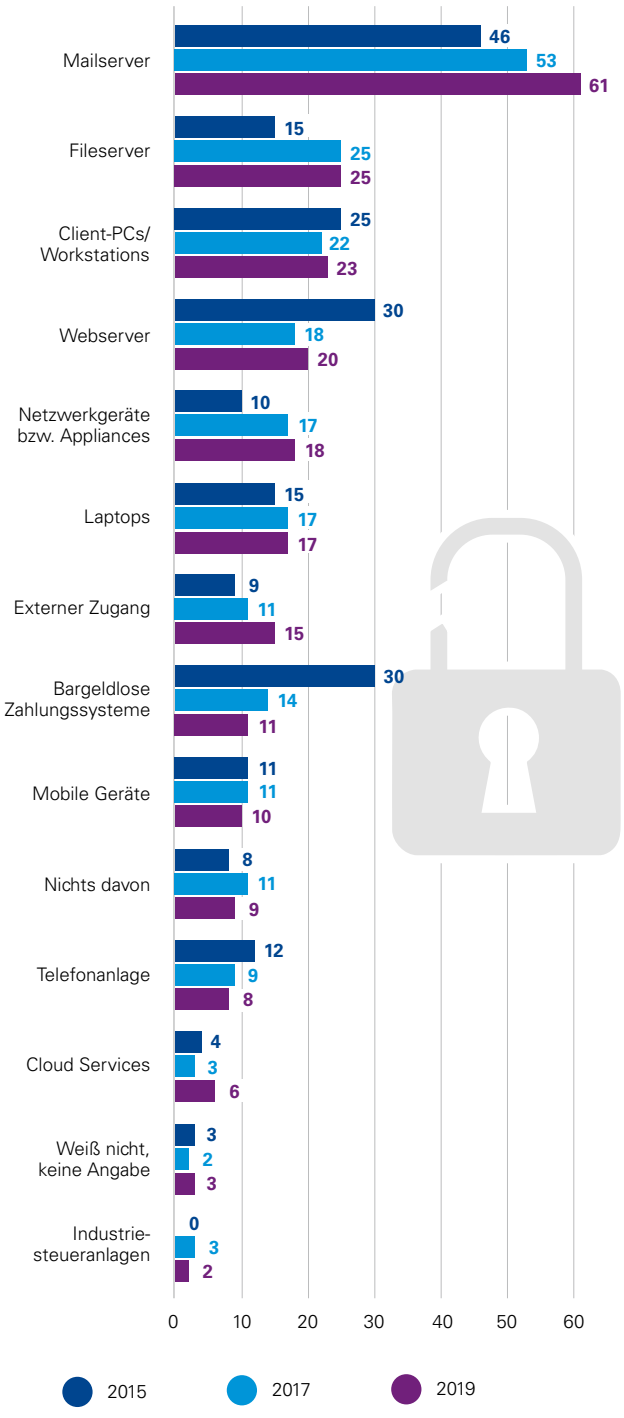
Quelle: KPMG in Deutschland, 2019

Die USA und Osteuropa werden in etwa so häufig wie bei der Befragung des Jahres 2017 von 15 beziehungsweise 13 Prozent der Studienteilnehmer genannt. Finanzdienstleister – die e-Crime grundsätzlich häufiger als andere Unternehmen in Verbindung mit bestimmten Ländern oder Regionen wahrnehmen (61 Prozent; allgemein: 52 Prozent) – sehen Osteuropa als besonders kritische Region (30 Prozent). Daneben wird Rumänien ausdrücklich von immerhin 10 Prozent der Vertreter des Finanzsektors genannt, möglicherweise aufgrund der aktuellen Geldwäscheskandale oder Fake-President-Fälle, die vielfach von Osteuropa ausgehen.

2.4. Angriffsziele

Mailserver sind das mit Abstand häufigste Angriffsziel von Computerkriminellen (61 Prozent; Abb. 8). Dieser Wert steigt kontinuierlich an (2015: 46 Prozent; 2017: 53 Prozent). Das unterstreicht, wie sehr Geschäftsverkehr und unternehmensinterne Abläufe inzwischen von der Nutzung von E-Mails abhängen und dass sich auf den zugehörigen Servern eine Vielzahl hochattraktiver Informationen befindet. Zudem sind beispielsweise Phishing-Mails eine verhältnismäßig unkomplizierte Methode, um einen Fuß in die Systemlandschaft eines Unternehmens zu bekommen. Auch der „Erfolg" von Deliktsarten wie Fake-President-Betrug und Ransomware-Angriffen ist zumeist darauf zurückzuführen, dass Kriminelle Mitarbeiter mit betrügerischen E-Mails zu folgenschweren Handlungen verleiten können.

Abb. 8: Angegriffene Systeme
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

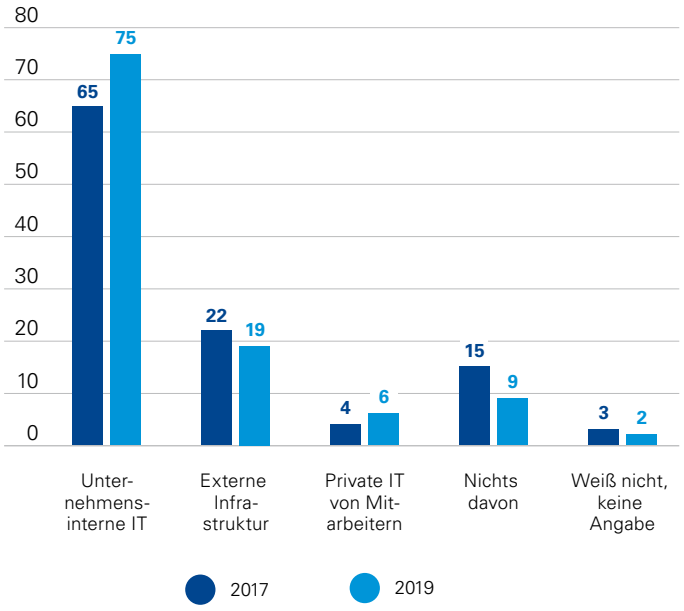
Umso wichtiger ist es, angemessene Maßnahmen zum Schutz von Mailservern zu ergreifen. Die in den vorigen Studien ermittelte Betroffenheit ließ darauf schließen, dass dies vor allem kleinen Unternehmen besonders schwer fiel. Auch heute sind Mailserver bei ihnen häufiger als bei den übrigen Befragten Ziel von Angriffen (67 Prozent). Allerdings hat der Abstand zu großen Unternehmen deutlich abgenommen. Bei diesen waren Mailserver in 53 Prozent der Fälle betroffen (2017: 39 Prozent), was zeigt, dass umsatzstarke Unternehmen derartige Angriffe ebenfalls nicht unterschätzen sollten.

Bei Fileservern zeigt sich ein deutlicherer Unterschied hinsichtlich der Unternehmensgröße: Die „Kleinen" sind prozentual doppelt so häufig betroffen wie die „Großen" (32 zu 16 Prozent). Umgekehrt müssen sich große Unternehmen wesentlich häufiger mit Angriffen auf Laptops auseinandersetzen (24 zu 14 Prozent), was darauf zurückzuführen sein könnte, dass sie ihren Mitarbeitern verhältnismäßig umfassend flexible Arbeitsplatzgestaltungen ermöglichen, in deren Rahmen in vielen Fällen nicht an stationären Rechnern gearbeitet, sondern ein eigenes mobiles Gerät genutzt wird. So sind Client-PCs und Workstations insbesondere bei kleinen Unternehmen häufig ein Angriffsziel (26 Prozent; große Unternehmen: 16 Prozent).

Gegenüber der Studie des Jahres 2017 lassen sich weitere Veränderungen kaum feststellen. Es ist allerdings festzuhalten, dass Unternehmen mit einer sehr ausgewogenen Gefahrenlage konfrontiert sind, wenn man die starke Gefährdung der Mailserver einmal außer Acht lässt. Neben den bereits erwähnten Angriffszielen werden auch Webserver und Netzwerkgeräte von über einem Sechstel der Betroffenen genannt. Es wäre daher leichtfertig, lediglich bestimmte Systeme zu schützen, denn nur umfassende Gegenmaßnahmen verhindern e-Crime effektiv.

Im Hinblick auf die betroffenen IT-Bereiche war nach wie vor insbesondere unternehmensinterne IT das hauptsächliche Angriffsziel bei e-Crime (75 Prozent; 2017: 65 Prozent). Lediglich jedes fünfte Unternehmen nennt externe Infrastrukturen und nur 6 Prozent die private IT von Mitarbeitern (Abb. 9).

Abb. 9: Angegriffene IT-Bereiche
Angaben in Prozent



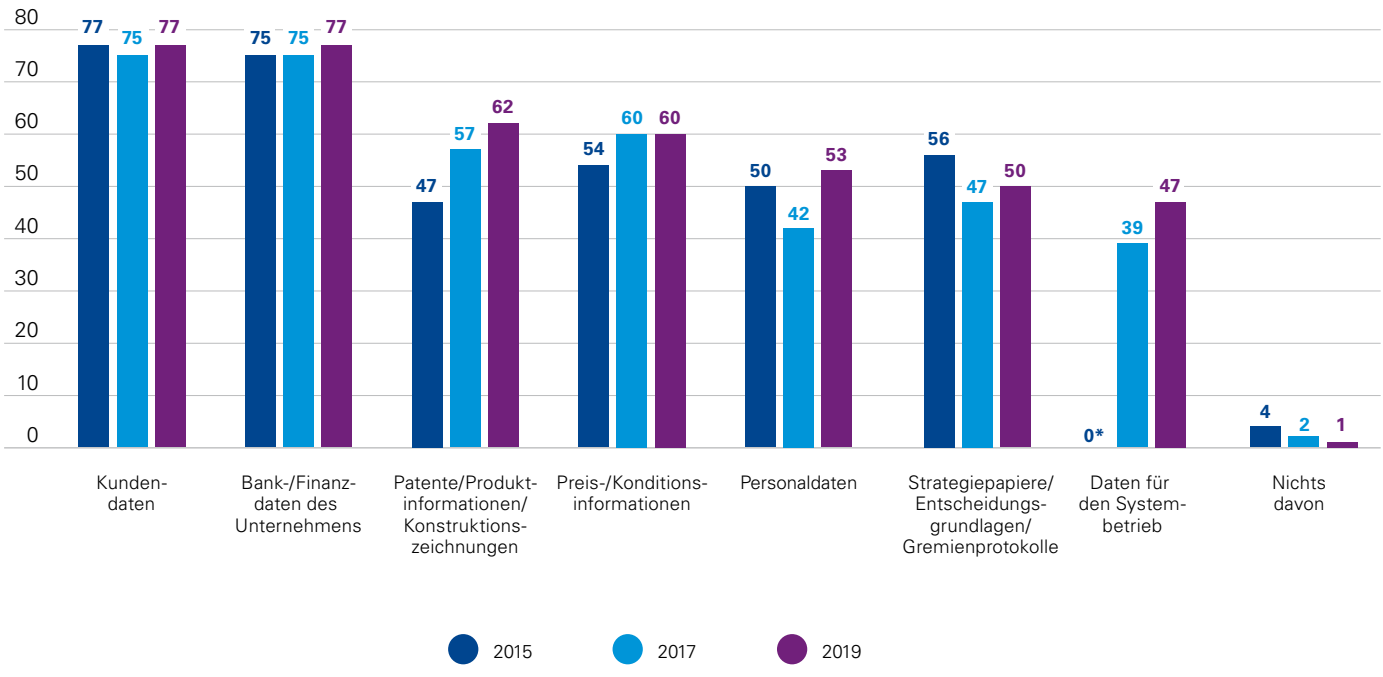
Quelle: KPMG in Deutschland, 2019

Je höher der Umsatz, desto stärker ist auch die Betroffenheit externer Infrastrukturen. So gibt knapp ein Drittel der großen Unternehmen eine Betroffenheit dieses Bereichs an (31 Prozent), unter den Finanzdienstleistern ist es sogar fast die Hälfte (46 Prozent). Dies könnte darin begründet sein, dass Unternehmen dieser Branche ihre IT-Strukturen vermehrt an externe Dienstleister auslagern. Zugleich gibt ein Viertel der Finanzdienstleister an, dass keiner der abgefragten IT-Bereiche angegriffen wurde. Dieser Wert könnte darauf zurückzuführen sein, dass beispielsweise kundenseitige IT-Anwendungen wie Online-Banking zwar von e-Crime betroffen waren, jedoch von den jeweiligen Befragten nicht der unternehmensexternen IT zugeordnet werden.

2.5. Risikobehaftete Informationen

Wie schon in den Vorgängerstudien bezeichnen gut drei Viertel der Befragten sowohl Bank- oder Finanz- als auch Kundendaten als besonders risikobehaftet im Hinblick auf e-Crime (Abb. 10). Kundendaten erachten insbesondere große Unternehmen und Finanzdienstleister als stark gefährdet (91 Prozent). Die schiere Menge an Daten stellt diese Unternehmen vor die Herausforderung, diese angemessen zu schützen und dabei Aspekte des Datenschutzes wie auch der Datensicherheit zu berücksichtigen. Gelingt dies nicht, bietet sich Kriminellen eine enorme Angriffsfläche, um solche Daten abzugreifen.

Abb. 10: Risikobehaftete Informationen
Angaben in Prozent

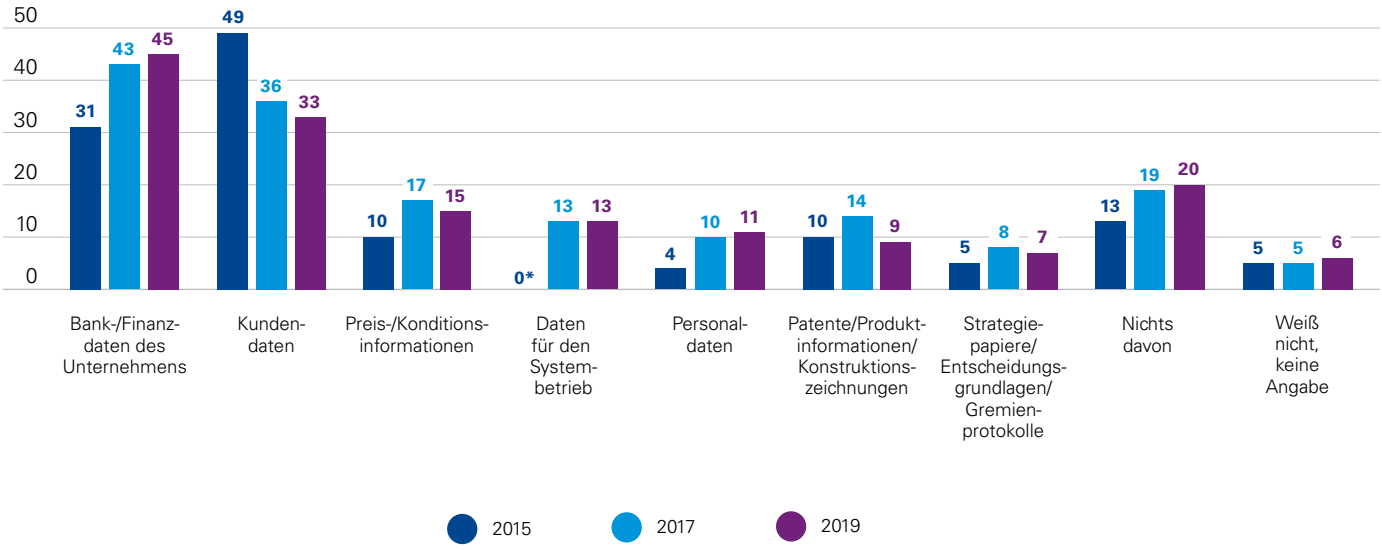


Quelle: KPMG in Deutschland, 2019

* Wurde 2015 nicht abgefragt.

Tatsächlich waren Kundendaten bei 45 Prozent der großen Unternehmen Ziel von e-Crime-Delikten und sind damit die meistbetroffene Datenart in dieser Unternehmenskategorie (kleine Unternehmen: 30 Prozent). Hingegen waren über alle Gruppen von Betroffenen hinweg zumeist Bank- oder Finanzdaten das Ziel Krimineller (45 Prozent; Abb. 11). Dies könnte erklären, weshalb bereits betroffene Unternehmen für diese Datenart ein geringfügig größeres Risiko wahrnehmen als nicht betroffene (81 zu 75 Prozent).

Abb. 11: Betroffene Informationsarten
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

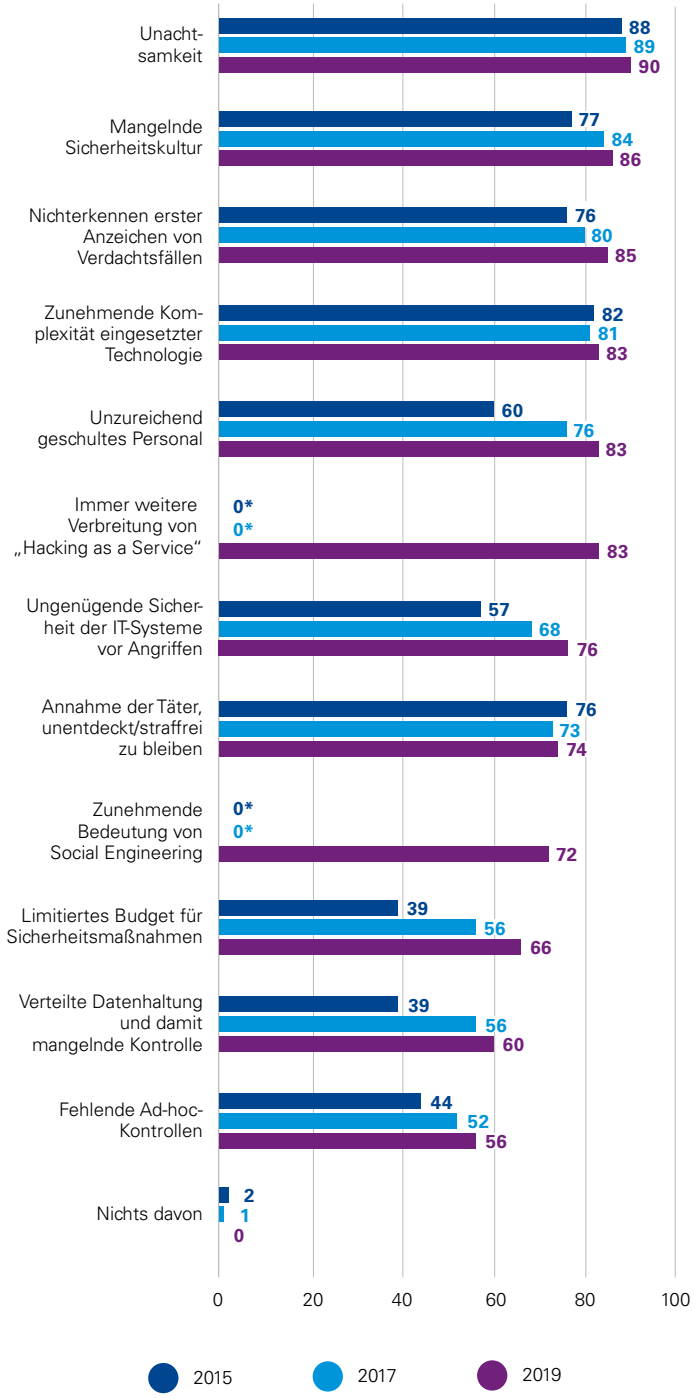
* Wurde 2015 nicht abgefragt.

Wie bei Kundendaten sehen umsatzstärkere Unternehmen auch bei Personaldaten ein höheres Risiko als die übrigen Befragten (60 Prozent; allgemein: 53 Prozent) – möglicherweise, da sie schlichtweg einen wesentlich höheren Aufwand betreiben müssen als kleine Unternehmen, um die Menge an Personaldaten zu erfassen und zu schützen. Die allgemeine Risikowahrnehmung hinsichtlich dieser Datenart ist darüber hinaus ebenfalls angestiegen (2019: 53 Prozent; 2017: 42 Prozent).

Preis- und Konditionsinformationen (60 Prozent) sowie Patente, Produktinformationen und Konstruktionszeichnungen (62 Prozent) betrachten etwa drei von fünf Befragten als besonders gefährdet. Für letztere Kategorie setzt sich somit der Trend der Vorgängerstudien fort (2015: 47 Prozent; 2017: 57 Prozent). Zudem lässt sich für Daten dieser Art eine branchenspezifische Risikowahrnehmung feststellen: In Industrieunternehmen gelten derartige Informationen als besonders risikobehaftet, auch wenn lediglich 9 Prozent dieser Unternehmen tatsächlich entsprechende Delikte vermelden.

Strategiepapiere, Entscheidungsgrundlagen oder Gremienprotokolle (50 Prozent) sowie Daten für den Systembetrieb (47 Prozent) sieht etwa die Hälfte als besonders risikobehaftet. Daten für den Systembetrieb stellen damit die vermeintlich am wenigsten gefährdete Datenart dar. Gleichwohl waren derartige Informationen immerhin in 13 Prozent der Fälle Ziel der Täter.

Abb. 12: Begünstigende Faktoren
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019 * Wurde in den Vorjahren nicht abgefragt.

2.6. Begünstigende Faktoren

Auch wenn es sich bei e-Crime um ein Phänomen handelt, von dem man annehmen könnte, dass es vor allem von technologischen Belangen abhängt, zeigt sich im Zuge der aktuellen Befragung erneut, dass menschliche Faktoren von größter Bedeutung sind.

So geben 90 Prozent der Befragten an, dass sie Unachtsamkeit als Faktor betrachten, der e-Crime besonders begünstigt (Abb. 12). Unachtsamkeit stellt dabei einen Aspekt dar, der vergleichsweise einfach abzustellen sein sollte, den man jedoch kaum gänzlich ausschließen kann. Ein Lösungsansatz besteht darin, die Mitarbeiter in Schulungen gezielt zu sensibilisieren, damit künftig die gebotene Sorge und Umsicht an den Tag gelegt werden.

Hier offenbart sich allerdings eines der zentralen Probleme: Zwar geben 88 Prozent der Befragten an, Maßnahmen zur Schulung und Sensibilisierung ihrer Mitarbeiter ergriffen zu haben, doch weisen gleichzeitig 83 Prozent unzureichend geschultes Personal als besonders risikobehafteten Faktor aus. Über die vergangenen Jahre hat dieser Punkt sogar an Bedeutung gewonnen (2015: 60 Prozent; 2017: 76 Prozent). In diesem Kontext bestehen offenbar größere Schwierigkeiten, unachtsames oder anderweitig leichtfertiges Verhalten effektiv einzudämmen. So entstehen Schwachstellen, die sich Computerkriminelle zunutze machen können.

Damit zusammenhängend benennen 86 Prozent der Teilnehmer eine mangelnde Sicherheitskultur einschließlich eines unzureichenden Risikoverständnisses. Dies ist besonders heikel, da ein grundlegendes Verständnis der relevanten Risiken Basisvoraussetzung dafür ist, angemessene präventive Maßnahmen zu treffen, erste Anzeichen von Vorfällen zu erkennen und im Ernstfall effektive Gegenmaßnahmen zu ergreifen – denn wer die grundlegende Gefahr nicht

versteht, wird nicht effektiv dagegen vorgehen können. Darüber hinaus unterstreicht dies die Wichtigkeit unternehmenskultureller Aspekte: Unternehmen müssen eine klare Kultur vorgeben, die nicht nur ethisch korrektes und gesetzestreues Verhalten fordert und fördert, sondern auch Umsicht und Sorgfalt im Umgang mit e-Crime propagiert. Diese Kultur muss von der Führungsebene (vor-)gelebt werden („Tone from the Top"), sodass Mitarbeiter ihr Verhalten daran ausrichten können.

Selbstverständlich sind in einem derart technologiebezogenen Feld wie dem der Computerkriminalität auch entsprechende Risikofaktoren von Belang. So betrachten jeweils fünf von sechs Befragten das Nichterkennen erster Anzeichen von Verdachtsfällen, eine zunehmende Komplexität der eingesetzten Technologie und die zunehmende Verbreitung von „Hacking as a Service" mit Sorge. Dabei ist nicht von der Hand zu weisen, dass die Komplexität und das Nichterkennen erster Anhaltspunkte untrennbar miteinander zusammenhängen. Gerade neuartige Technologien werden häufig zum Einfallstor für Computerkriminelle, da in vielen Fällen im angegriffenen Unternehmen noch keine angemessenen Sicherheitsmaßnahmen existieren und es Mitarbeitern möglicherweise noch an einem tiefgreifenden Verständnis einzelner Maßnahmen und Prozesse fehlt. So benennen immerhin drei Viertel der Befragten als begünstigenden Faktor für computerkriminelle Handlungen, dass IT-Systeme vor Angriffen ungenügend gesichert waren. Es ist daher durchaus möglich, dass Anzeichen von Angriffen bei weniger komplexen Technologien, bei denen eine gewisse Routine im Umgang gegeben ist, eher festgestellt werden. Unternehmen müssen also dafür sorgen, dass sich alle Beteiligten kontinuierlich mit der Funktionsweise und den damit verbundenen Möglichkeiten und Risiken neuartiger Technologien vertraut machen. Dies ist umso dringlicher, als das Nichterkennen erster Anzeichen im Ernstfall sogar bedeuten kann, dass e-Crime-Schäden kaum noch abzuwenden sind. Angesichts dieser Tatsache überrascht es nicht, dass die Befragten diesem Faktor eine immer höhere Wichtigkeit beimessen (2015: 76 Prozent; 2017: 80 Prozent; 2019: 85 Prozent).

Unternehmen erkennen zudem, dass die mit Computerkriminalität verbundene Anonymität ebenfalls ein bedeutender Anreiz für potenzielle Täter ist. Knapp drei Viertel der Befragten führen die Annahme der Täter, unentdeckt zu bleiben, als einen Faktor an, der e-Crime begünstigt.

Darüber hinaus sind neuartige Phänomene wie das schon angesprochene „Hacking as a Service" (83 Prozent) und die zunehmende Rolle von Social Engineering (72 Prozent) im Fokus der Studienteilnehmer. Ersteres ist insbesondere deswegen relevant, da es auch technisch unbegabten Tätern die Möglichkeit gibt, e-Crime sozusagen als Dienstleistung einzukaufen. Das Feld potenzieller Täter ist daher kaum noch einzugrenzen, denn wer über die entsprechende Motivation verfügt, kann auch an die erforderlichen Ressourcen gelangen.

Bei Social Engineering handelt es sich um ein Phänomen, das vor allem in Bezug auf Phishing und CEO Fraud verstärkt in den Blick gerückt ist. Hierbei sammeln Kriminelle zunächst Informationen über ein potenzielles Opfer und spionieren über öffentlich zugängliche Quellen und soziale Netzwerke sein persönliches Umfeld aus. So können sie sich im nächsten Schritt mit täuschend echten E-Mails oder Anrufen an die Zielperson wenden, um sie beispielsweise zur Preisgabe vertraulicher Informationen oder – wenn es zahlungsberechtigte Mitarbeiter sind – zu Zahlungsanweisungen für vermeintlich geheime Projekte zu verleiten.

Die Beobachtung aus den vorigen Studien, dass die Befragten einige grundlegende Faktoren zunehmend kritisch betrachten, wird mit den Ergebnissen der neuesten Befragung bestärkt. So nennen sie ein limitiertes Budget (2017: 56 Prozent; 2019: 66 Prozent), verteilte Datenhaltung (2017: 56 Prozent; 2019: 60 Prozent) und auch fehlende Ad-hoc-Kontrollen (2017: 52 Prozent; 2019: 56 Prozent) allesamt häufiger als 2015 und 2017. Dass es Unternehmen dabei insbesondere vermehrt an finanziellen Mitteln für angemessene Sicherheitsmaßnahmen mangelt, ist besonders problematisch, zeigt sich allerdings auch bei den abgefragten Investitionsvolumina. Vor allem im Feld der Computerkriminalität kommt kein Unternehmen umhin, für die neuesten Herausforderungen jederzeit angemessene Gegenmaßnahmen aufzubieten. Wer mit der stetigen Weiterentwicklung der Technologie und krimineller Angriffsmuster nicht mithält, wird gravierende Schäden nicht dauerhaft verhindern können. Wirksame Gegenmaßnahmen erfordern allerdings merkliche Investitionen. Mögen diese zwar zunächst kostspielig erscheinen, sind sie dennoch von beträchtlichem – auch finanziellem – Nutzen, da sie entstehende Schäden erheblich mindern oder sogar gänzlich verhindern können. Die auf diese Weise vermiedenen finanziellen Schäden dürften Implementierungs- und Instandhaltungskosten von Präventionsmaßnahmen in der Regel überwiegen, womit diese letztlich ein Gewinn sind. e-Crime-Prävention ist somit immer auch Ausdruck ökonomisch motivierten Handelns.

2.7. Kosten

In dieser Studie wird auf die Angabe eines Durchschnittswerts, der die durch e-Crime insgesamt verursachten Schäden beziffert, verzichtet. Stattdessen sind Bereiche angegeben, in denen sich die jeweiligen Schadenssummen in der Regel einordnen lassen (50-Prozent-Quartil um den Median). Dies führt zu aussagekräftigeren Zahlen, da Extremwerte die Berechnung eines Durchschnitts erheblich verzerren können. Um allerdings Extreme ebenfalls zu berücksichtigen, wird im Folgenden auf bestimmte Ausreißer separat eingegangen. Auf diesem Weg sind präzisere Einschätzungen der zu erwartenden Schadenssummen möglich.

Der in den vergangenen zwei Jahren durch e-Crime verursachte Gesamtschaden der Betroffenen hat sich gegenüber den Angaben der vorangegangenen Studie lediglich geringfügig verändert. Bei den mittleren 50 Prozent der Unternehmen lag er zwischen 20.000 und 150.000 Euro. Es ist allerdings nicht unüblich, dass Unternehmen sogar Schadenssummen von 500.000 Euro oder mehr verzeichnen (14 Prozent aller Unternehmen, die eine Schadenssumme angeben). Bei knapp 7 Prozent der Betroffenen belief sich der Gesamtschaden sogar auf 1 Million Euro oder mehr (2017: 5 Prozent). Etwas mehr als ein Viertel der Befragten konnte oder wollte keine Angabe im Rahmen dieser Fragestellung machen.

Gesamtschaden nach Unternehmensgröße, gemessen am Umsatz*				
	Gesamt	Umsatz unter 250 Mio. Euro	Umsatz zwischen 250 Mio. und 3 Mrd. Euro	Umsatz über 3 Mrd. Euro
Anzahl (absolut)	278	126	116	36
Niedrig (unter 10.000 Euro)	8,33 %	14,86 %	2,90 %	0,00 %
Mittel (10.000 bis 99.999 Euro)	51,39 %	60,81 %	44,93 %	39,73 %
Hoch (100.000 bis 999.999 Euro)	33,33 %	24,32 %	42,03 %	39,73 %
Sehr hoch (1.000.000 Euro oder mehr)	6,94 %	1,35 %	10,14 %	21,92 %

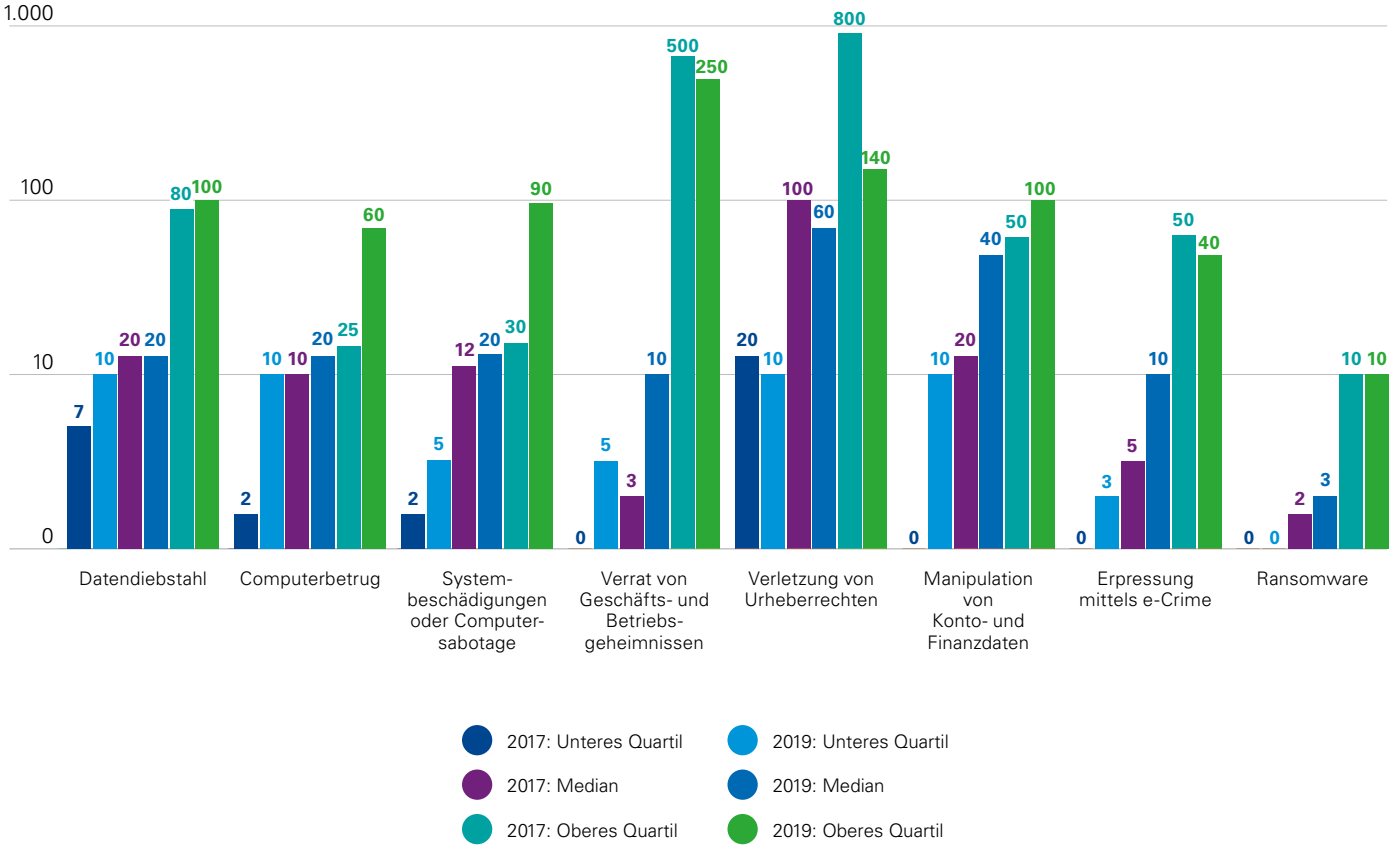
* Bei den Prozentangaben sind Rundungsdifferenzen möglich.

Schäden in Millionenhöhe wurden auch für jede einzelne abgefragte Deliktsart genannt. Hierin zeigt sich die Vielschichtigkeit der e-Crime-Gefahrenlage.

Die meisten deliktsspezifischen Schadenssummen haben sich leicht erhöht. So lagen in der vorigen Studie etwa 50 Prozent der Schäden durch Systembeschädigung und Computersabotage zwischen 2.000 und 30.000 Euro, dieses Jahr liegen sie zwischen 5.000 und 90.000 Euro. Bei der Manipulation von Konto- und Finanzdaten lagen in der der vorigen Studie die mittleren 50 Prozent aller genannten Schadenssummen zwischen 1.000 und 50.000 Euro, in der diesjährigen nun zwischen 10.000 und 100.000 Euro (Abb. 13).

Der Gesamtschaden beinhaltet die Gesamtheit aller durch computerkriminelle Handlungen abgeflossenen Vermögenswerte, den entgangenen Gewinn, Ermittlungs- und Folgekosten, Bußgelder, Geldstrafen und eventuelle Gewinnabschöpfungen.

Abb. 13: Vergleich Gesamtschaden
Angaben in Tausend Euro



Quelle: KPMG in Deutschland, 2019

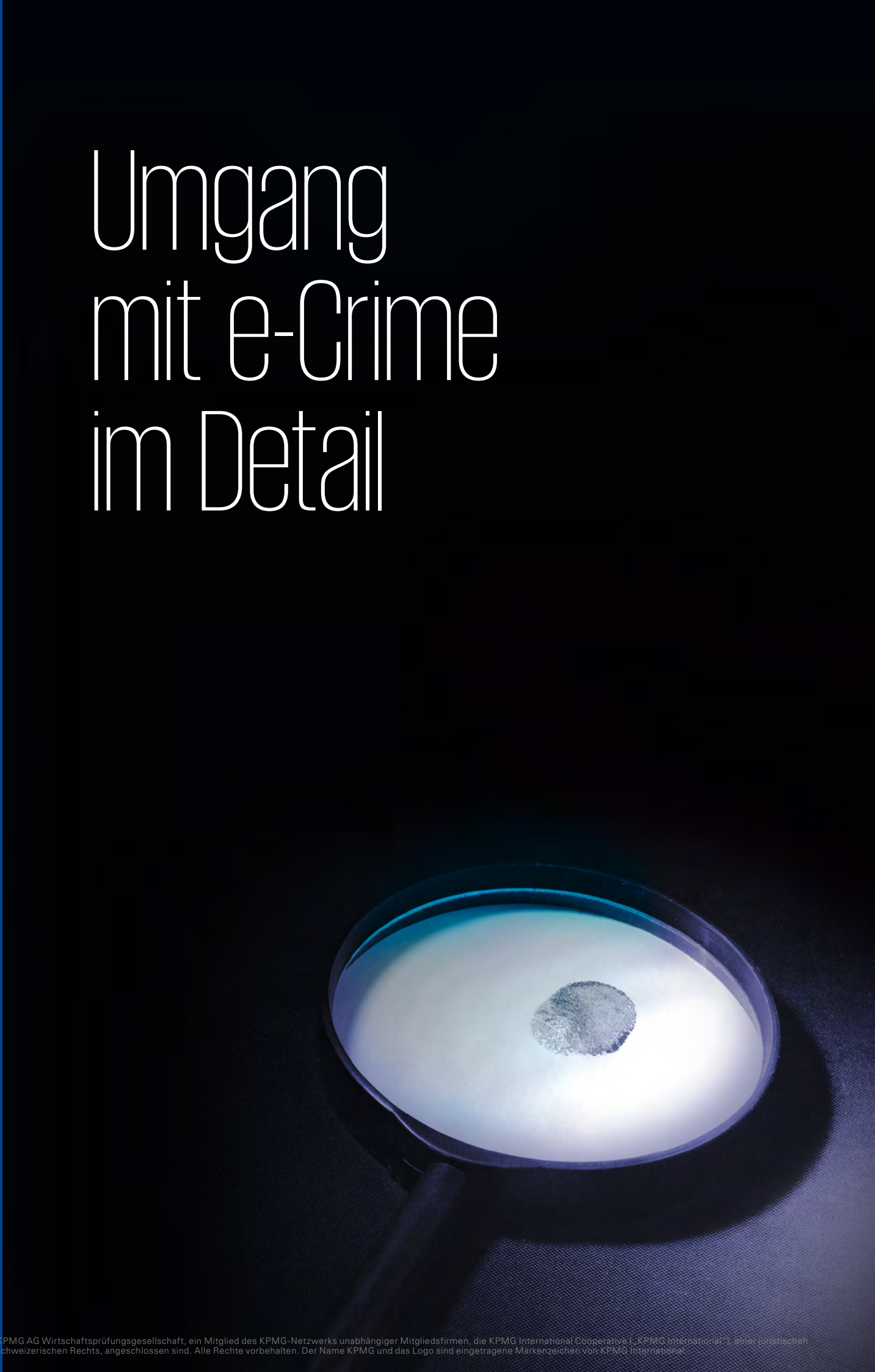
Eine gegenläufige Tendenz zeigt sich im Zusammenhang mit der Verletzung geistigen Eigentums. Zwar verursachen derartige Taten nach wie vor unter allen Deliktsarten die höchsten Gesamtschäden, doch sind diese gegenüber den Ergebnissen der vergangenen Befragung deutlich gesunken. So waren 2017 bei der Verletzung von Geschäftsgeheimnissen Kosten von 500.000 Euro durchaus im Rahmen des Erwartbaren (oberes Quartil) und bei der Verletzung von Urheberrechten wurden sogar Schäden in Höhe von 800.000 Euro berichtet. Dieses Jahr liegen die entsprechenden Schadenssummen jedoch „nur" bei 250.000 beziehungsweise 140.000 Euro. Eine Erklärung könnte im größeren Umfang der Stichprobe liegen – dieses Jahr wurde die doppelte Anzahl an Unternehmen befragt. Hinzu kommt, dass diese beiden Deliktsarten ohnehin zu den seltener genannten computerkriminellen Handlungen gehören und 2017 somit selbst die mittleren 50 Prozent der Schadenssummen nah an den Extremwerten lagen.

Neben den Gesamtschäden erfasst diese Befragung auch die angefallenen Ermittlungs- und Folgekosten, die bei der Mehrheit der abgefragten Deliktsarten etwa ein Drittel des Gesamtschadens ausmachen (Abb. 14). Ausnahmen sind hier die Verletzung von Geschäftsgeheimnissen (16 Prozent), Computerbetrug (42 Prozent) und die Verletzung von Urheberrechten (43 Prozent).

Abb. 14: Anteil der Ermittlungs- und Folgekosten am Gesamtschaden
Angaben in Prozent

Quelle: KPMG in Deutschland, 2019

Umgang mit e-Crime im Detail



03 Prävention, Detektion und Reaktion

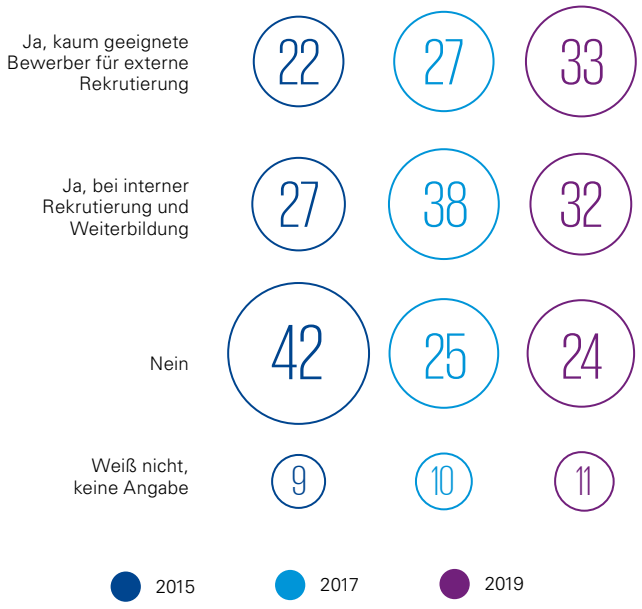
3.1. Prävention

3.1.1. Verfügbarkeit von Personal

Die Gewinnung geeigneten Personals und die Weiterbildung der Belegschaft sind bei der Bekämpfung von e-Crime ein besonders bedeutsamer Erfolgsfaktor. Nicht umsonst nennen fünf von sechs Befragten unzureichend geschultes Personal als Antwort auf die Frage, welche Aspekte die Anfälligkeit für Computerkriminalität besonders prägen. Es ist daher darauf zu achten, dass die Mitarbeiter die erforderlichen Qualifikationen besitzen, um e-Crime einerseits präventiv entgegenzutreten, im Ernstfall aber auch Angriffe angemessen aufzuklären.

In der diesjährigen Studie stellt es für zwei Drittel der Unternehmen eine massive Herausforderung dar, kompetentes Personal zu rekrutieren oder in den eigenen Reihen weiterzubilden (Abb. 15). Auffällig im Vergleich zu den Ergebnissen der Studie des Jahres 2017 ist insbesondere, dass sich die Schwierigkeiten zwischen interner und externer Rekrutierung nun etwa die Waage halten, wohingegen in der vorigen Studie ein deutliches Übergewicht bei der Herausforderung bestand, intern Personal zu gewinnen und weiterzubilden. So verwies in diesem Jahr jeweils ein knappes Drittel der Unternehmen auf Probleme bei der internen Rekrutierung und Weiterbildung (2017: 38 Prozent) und bei der externen Rekrutierung (2017: 27 Prozent).

Abb. 15: Herausforderung bei der Akquise qualifizierten Personals
Angaben in Prozent



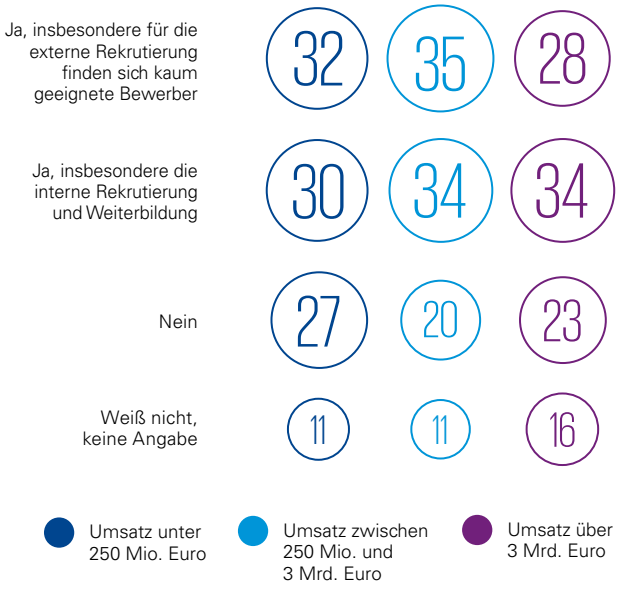
Quelle: KPMG in Deutschland, 2019

Bei der Betrachtung der Unternehmen nach Umsatz zeigt sich, dass immerhin knapp jedes dritte große Unternehmen die interne Rekrutierung kritisch sieht (Abb. 16), dieser Wert jedoch im Vergleich zur vorherigen Befragung um 10 Prozentpunkte zurückgegangen ist. Hingegen nimmt nun etwas mehr als jedes vierte große Unternehmen Herausforderungen bei der externen Rekrutierung geeigneter Bewerber wahr. Im Vergleich zu 2017 bedeutet dies einen Anstieg von 19 auf 28 Prozent. Eine ähnliche Entwicklung ist bei den mittleren Unternehmen festzustellen.

Bei kleineren Unternehmen bezeichnet knapp jeder dritte Befragte die externe wie auch die interne Rekrutierung als Herausforderung. Bemerkenswert ist allerdings, dass mehr als jedes vierte kleine Unternehmen gar keine Herausforderungen bei der Akquise qualifizierten Personals sieht.

Zudem fällt auf, dass von e-Crime betroffene Unternehmen geringere Schwierigkeiten bei der Personalakquise sehen als nicht betroffene – mehr als ein Viertel der Betroffenen empfindet sie nicht als Herausforderung. Dies zeigte sich bereits in der vorigen Studie und kann in zweierlei Hinsicht interpretiert werden: Einerseits könnte es darauf schließen lassen, dass die Betroffenen die e-Crime-Risiken weiterhin unterschätzen; andererseits könnte es auch bedeuten, dass betroffene Unternehmen mehr Geld in die Hand nehmen, was die Personalgewinnung erleichtern dürfte.

Abb. 16: Herausforderungen bei der Akquise qualifizierten Personals nach Unternehmensgröße
Angaben in Prozent



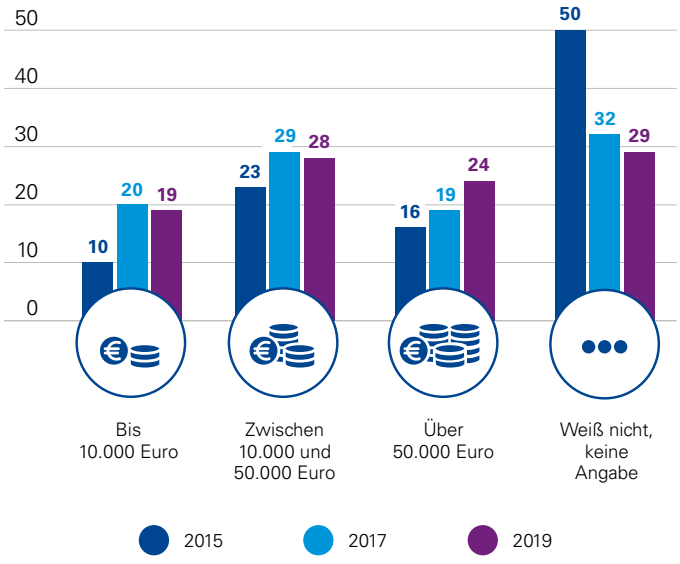
Quelle: KPMG in Deutschland, 2019

3.1.2. Aktuelle und geplante Investitionen

Nach den jährlichen Investitionen in e-Crime-Prävention, -Erkennung und -Reaktion gefragt, machen 29 Prozent der Unternehmen keine Angaben. Diese Zahl ist durchaus hoch und könnte vermuten lassen, dass Unternehmen ihre Ausgaben in diesem Bereich nicht angemessen steuern können. Ist dies der Fall, wird es zunehmend schwierig, die Effizienz der getroffenen Maßnahmen zu beurteilen. Dabei ist es angesichts vergleichsweise geringer Investitionsvolumina besonders wichtig, die bereitstehenden Mittel effektiv und kosteneffizient einzusetzen.

Dennoch setzt sich der positive Trend der vorangegangenen Studien fort, wenn auch in deutlich geringerem Maße. Konnte – oder wollte – im Jahr 2015 jedes zweite Unternehmen keine Angaben zu den jährlichen Investitionen machen, war es nun „nur" jedes dritte.

Abb. 17: Investitionen in e-Crime-Bekämpfung nach Jahr
Angaben in Prozent

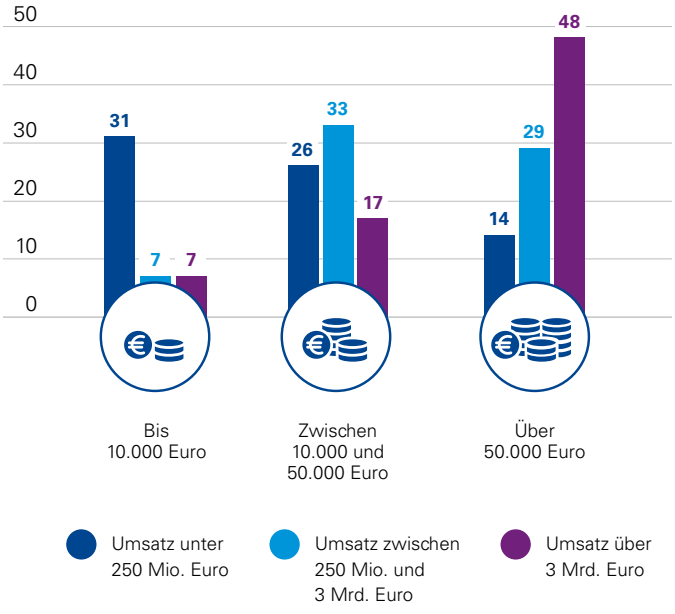


Quelle: KPMG in Deutschland, 2019

Die angegebenen Investitionsvolumina sind nach wie vor eher bescheiden. Beispielsweise gibt jedes fünfte Unternehmen jährlich weniger als 10.000 Euro für die Bekämpfung von e-Crime aus (Abb. 17). Dies dürfte ob der vielfältigen Risiken der Computerkriminalität kaum ausreichen, um sich angemessen zu schützen und im Ernstfall entsprechende Gegenmaßnahmen zu ergreifen. Betroffene Unternehmen haben dieses Defizit offenbar erkannt und ihre Lehren daraus gezogen, denn sie investieren höhere Beträge als diejenigen, die bisher nicht betroffen waren. So gibt immerhin jedes dritte der betroffenen Unternehmen über 50.000 Euro jährlich aus, bei den übrigen Befragten tut dies nur etwa jedes fünfte.

Wenig überraschend ist, dass mit steigendem Umsatz eines Unternehmens auch die Investitionsbereitschaft zunimmt. So beziffert knapp jeder zweite „Große“ seine Investitionssumme auf über 50.000 Euro jährlich (Abb. 18). Von den „Kleinen“ nennen nur 14 Prozent diesen Bereich, bei den mittleren Unternehmen sind es 29 Prozent. Der größte Anteil (33 Prozent) der mittleren Unternehmen gibt an, dass die Investitionen zwischen 10.000 und 50.000 Euro liegen. Knapp jedes dritte kleine Unternehmen (31 Prozent) investiert hingegen nur bis zu 10.000 Euro.

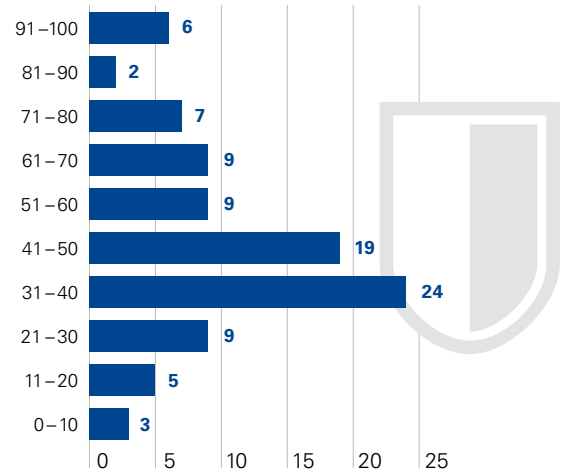
Abb. 18: Investitionen in e-Crime-Bekämpfung nach Umsatz
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

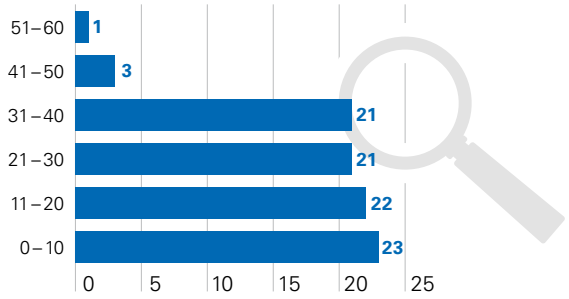
Insbesondere bei bereits betroffenen Unternehmen überwiegen Investitionen in die Prävention gegenüber Ausgaben für Aufdeckung, Aufklärung und Reaktion. Mehr als jedes zweite Unternehmen dieser Gruppe (58 Prozent) verwendet zwei Fünftel der jährlichen Gesamtausgaben für die Prävention. Bei den nicht betroffenen Unternehmen gilt dies nur für 48 Prozent. Betroffene Unternehmen erkennen also eher an, dass nur durch den Einsatz entsprechender Ressourcen für vorbeugende Maßnahmen e-Crime effektiv angegangen werden kann. Beispielsweise bieten sich Schulungen zur Sensibilisierung von Mitarbeitern, Fortbildungen für interne Taskforce-Monitoringsysteme, Datenanalysen, IT-Forensik oder Verträge mit externen Dienstleistern an, um Schwachstellen auszuräumen.

Abb. 19: Prozentuale Verteilung des jährlichen Investitionsvolumens auf den Bereich Prävention
Angaben in Prozent



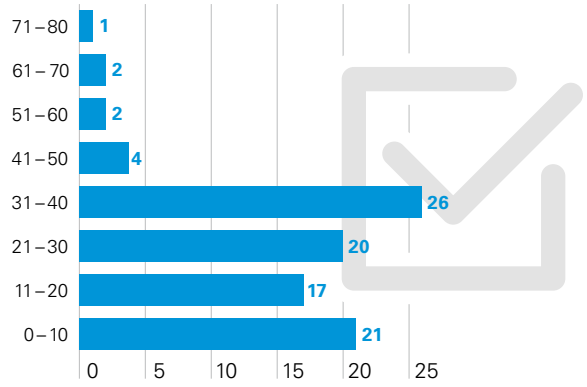
Quelle: KPMG in Deutschland, 2019

Abb. 20: Prozentuale Verteilung des jährlichen Investitionsvolumens auf den Bereich Aufdeckung und Aufklärung
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Abb. 21: Prozentuale Verteilung des jährlichen Investitionsvolumens auf den Bereich Reaktion
Angaben in Prozent

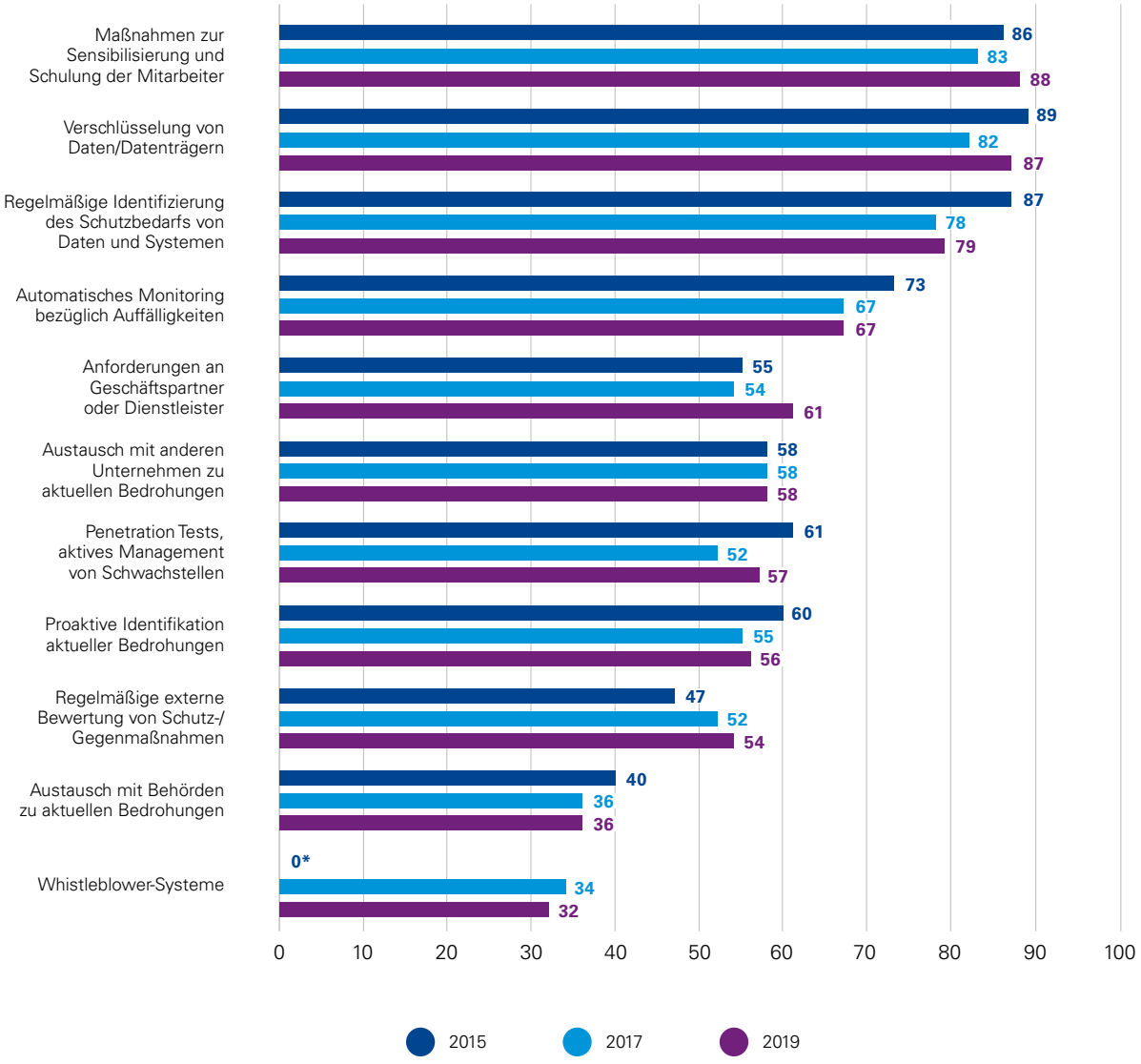


Quelle: KPMG in Deutschland, 2019

Insgesamt nutzt etwa jedes zweite Unternehmen zwischen 30 und 60 Prozent der jährlichen Investitionsvolumina für die Prävention (Abb. 19) sowie bis zu 20 Prozent für Aufdeckung und Aufklärung (Abb. 20). Die Ausgaben für Reaktionsmaßnahmen liegen mehrheitlich zwischen 20 und 40 Prozent (Abb. 21).

Wie auch in der vorangegangenen Studie festgestellt, will etwas mehr als jedes zweite Unternehmen (55 Prozent) die Investitionen in die Bekämpfung von e-Crime erhöhen, 3 Prozent planen sogar eine starke Erhöhung. Knapp zwei von fünf Unternehmen geben an, die Ausgaben in der bisherigen Höhe belassen zu wollen.

Abb. 22: Implementierte Präventionsmaßnahmen
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

* Wurde 2015 nicht abgefragt.

3.1.3. Maßnahmen zur Prävention

Nachdem 2017 zu konstatieren war, dass die Studienteilnehmer die abgefragten Präventionsmaßnahmen größtenteils seltener umgesetzt hatten als noch 2015, kehrt sich dieser Trend nun wieder um (Abb. 22). Insbesondere die Verschlüsselung von Daten und Datenträgern, Maßnahmen zur Sensibilisierung und Schulung der Mitarbeiter sowie Penetration Tests wurden von den Befragten jeweils um 5 Prozentpunkte häufiger genannt als zuvor. Den Unternehmen ist darüber hinaus zunehmend wichtig, dass Geschäftspartner oder Dienstleister gezielte Vorgaben zur e-Crime-Prävention befolgen (2017: 54 Prozent; 2019: 61 Prozent). In Betracht kommen beispielsweise die Verschlüsselung der E-Mail-Kommunikation oder auch zusätzliche Maßnahmen zur Sicherstellung der Datensicherheit.

Die drei meistgenannten Maßnahmen sind die gleichen wie in der vorigen Befragung: Sensibilisierung und Schulung der Mitarbeiter (88 Prozent), Verschlüsselung von Daten und Datenträgern (87 Prozent) sowie regelmäßige Identifizierung des Schutzbedarfs von Daten und Systemen (79 Prozent).

Wie die Studienergebnisse illustrieren, sind Unachtsamkeit, eine unzureichende Schulung der Belegschaft sowie die grundsätzliche Herausforderung, qualifiziertes Personal zu finden, dominierende Risikofaktoren. Dies unterstreicht die Bedeutung entsprechender Schulungen, der die Befragten in der Praxis mittlerweile durchaus Rechnung tragen.

Mit Blick auf den immer größeren Wert von Daten als Rohstoff eines Unternehmens ist es ebenfalls unerlässlich, Daten wie auch Datenträger angemessen zu verschlüsseln. Im Falle eines Datenlecks drohen Unternehmen nicht nur finanzielle Einbußen, sondern teils auch erhebliche Reputationsschäden. Unabdingbar sind hier die regelmäßige Identifikation des Schutzbedarfs von Daten und Systemen und die gegebenenfalls erforderliche Anpassung der bisherigen Maßnahmen. Dies ist vor allem deshalb relevant, da sich e-Crime-Delikte stetig weiterentwickeln und Cyber-Kriminelle immer wieder neue Methoden anwenden. Hier ist erneut auf die in den vergangenen Jahren gestiegene Gefahr von Ransomware zu verweisen.

Weitere besonders häufig genannte Präventionsmaßnahmen sind Anforderungen an Geschäftspartner wie auch das automatische Monitoring bezüglich Auffälligkeiten, die von etwas mehr als zwei Dritteln der Befragten angegeben werden. Der Großteil der weiteren abgefragten Maßnahmen wird von etwas mehr als der Hälfte der Studienteilnehmer angeführt.

Bei der Betrachtung der verschiedenen Umsatzklassen zeigt sich – wenig überraschend –, dass umsatzstärkere Unternehmen über einen größeren Maßnahmenkatalog verfügen als umsatzschwächere. Besonders deutlich wird dies bei der Einrichtung von Whistleblowing-Systemen: Während knapp zwei Drittel der „Großen“ über ein solches System verfügen, trifft dies nur auf etwa ein Fünftel der „Kleinen“ zu.

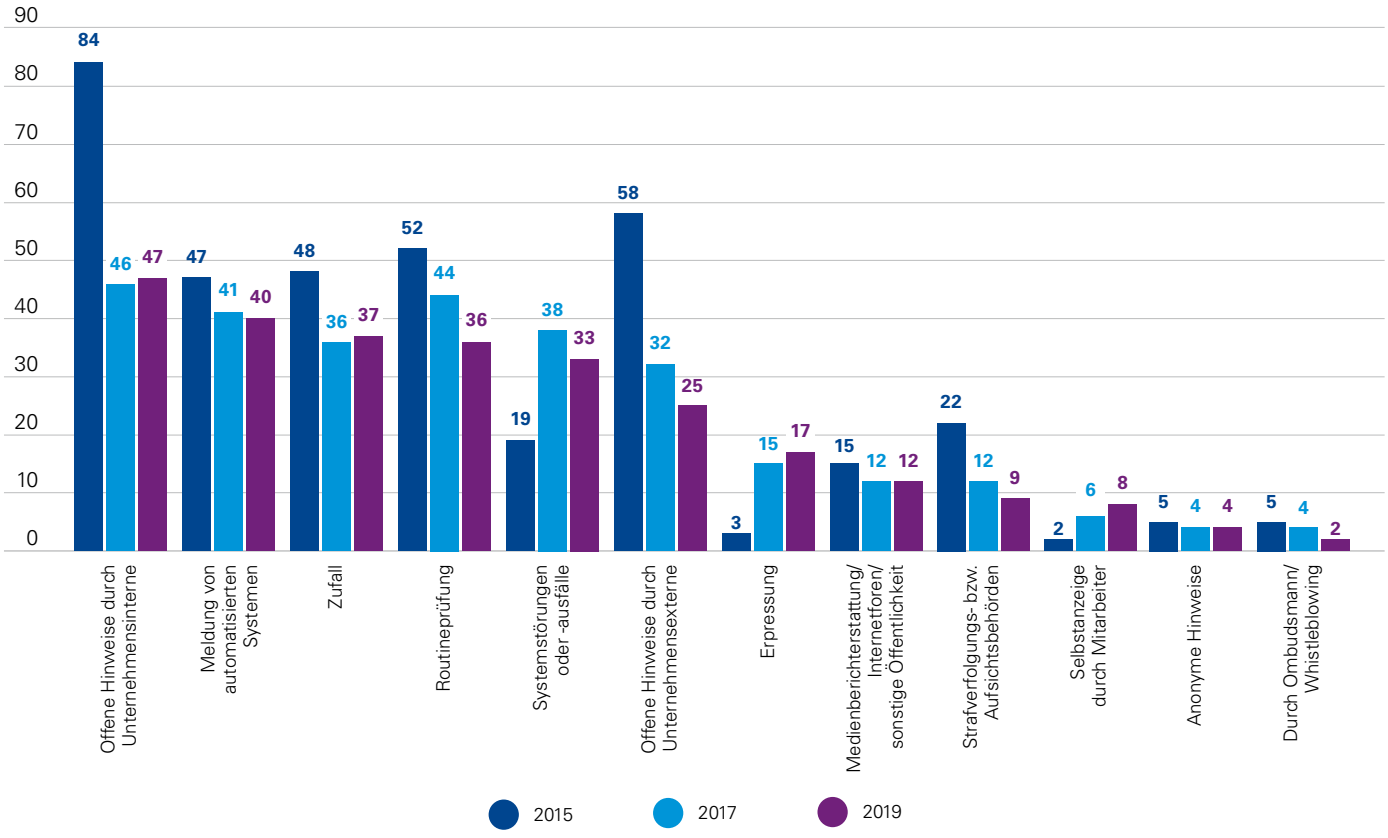
Finanzdienstleister sind im Branchenvergleich wesentlich besser aufgestellt als die übrigen Befragten. Dies zeigte sich schon in den Studien von 2015 und 2017 und dürfte vor allem in den hohen regulatorischen Anforderungen dieses Sektors begründet sein. Hinzu kommt, dass die meisten Unternehmen dieses Bereichs vergleichsweise umsatzstark sind.

3.2. Aufdeckung und Aufklärung

3.2.1. Entdeckung der Handlung

Im Vergleich zur Studie des Jahres 2017 zeigen sich nur unwesentliche Veränderungen im Hinblick auf die Entdeckung von e-Crime (Abb. 23). Nennenswerte Unterschiede lassen sich lediglich für offene Hinweise durch Unternehmensexterne (2017: 32 Prozent; 2019: 25 Prozent) und Hinweise aus Routineprüfungen (2017: 44 Prozent; 2019: 36 Prozent) feststellen.

Abb. 23: Entdeckung der Handlung
Angaben in Prozent

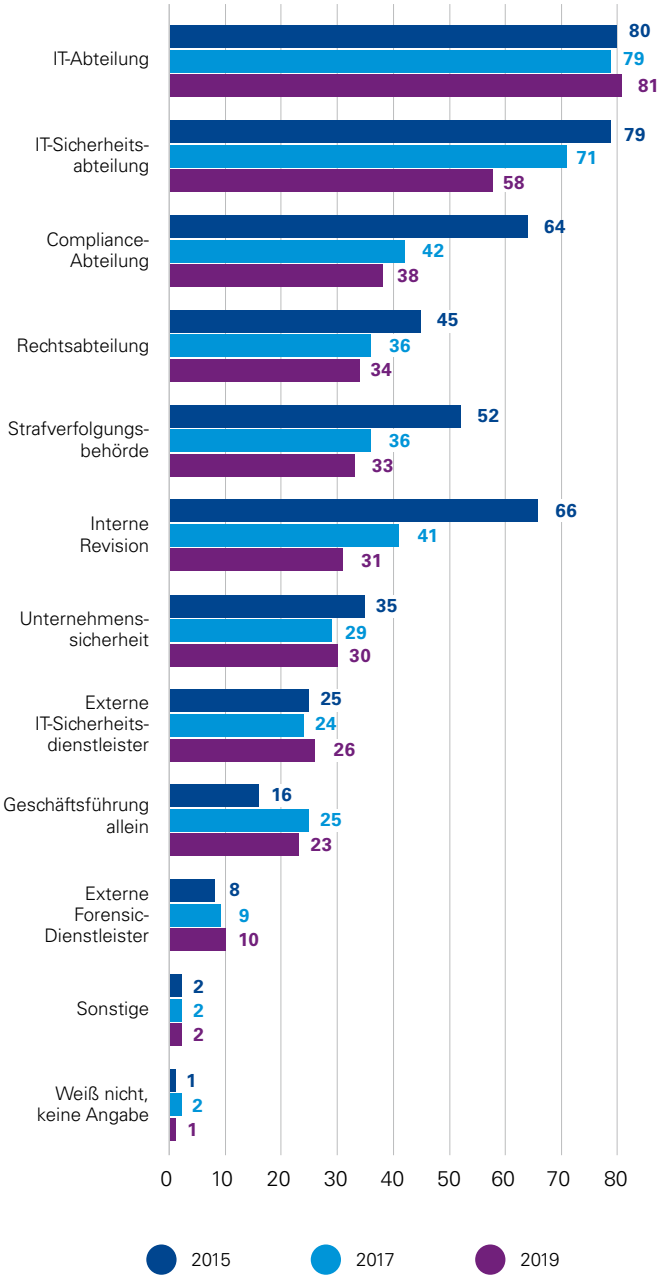


Quelle: KPMG in Deutschland, 2019

Zumeist wurden die Betroffenen durch offene Hinweise Unternehmensinterner (47 Prozent) oder die Meldung von automatisierten Systemen (40 Prozent) auf e-Crime-Vorfälle aufmerksam gemacht. Hinweise von Beschäftigten stehen somit bei der Aufdeckung an erster Stelle, gefolgt vor allem von technologie- und prozessbedingten Hinweisen wie solchen aus automatisierten Systemen oder Routineprüfungen sowie Systemstörungen oder -ausfällen (33 Prozent).

Nach wie vor wurde mehr als ein Drittel aller Fälle zufällig entdeckt (2017: 36 Prozent; 2019: 37 Prozent) – eine bedenklich hohe Zahl. Sie unterstreicht, dass die Detektion computerkrimineller Handlungen für Unternehmen eine große Herausforderung bedeutet und vielfach schlicht von Glück abhängt. Insofern gibt es erneut Anlass zu der Annahme, dass viele Delikte in einem Dunkelfeld geschehen.

Abb. 24: Operative Aufklärung
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Etwas mehr als jeder sechste Betroffene wurde durch Erpressung auf e-Crime aufmerksam gemacht, was häufig im Zusammenhang mit Ransomware-Angriffen der Fall ist.

Ein Drittel der größeren Unternehmen hat e-Crime-Vorfälle aufgrund offener Hinweise durch Externe wie Kunden oder Geschäftspartner entdeckt. Bei den kleineren Unternehmen trifft dies jedoch nur auf maximal jedes vierte zu, vermutlich deswegen, da sie schlichtweg mit weniger Dritten zusammenarbeiten. Wenig überrascht zudem, dass große Unternehmen vergleichsweise viele Hinweise von Strafverfolgungs- und Aufsichtsbehörden erhalten (16 Prozent). Dies gilt nur für 4 Prozent der kleinen und 11 Prozent der mittleren Unternehmen.

3.2.2. Operative Aufklärung

Die operative Aufklärung eines e-Crime-Delikts erfolgt nach wie vor hauptsächlich durch die unternehmenseigene IT-Abteilung (81 Prozent). Die IT-Sicherheitsabteilung, vor zwei Jahren noch von 71 Prozent der betroffenen Unternehmen mit der Aufklärung betraut, nennen in der diesjährigen Befragung hingegen nur noch 58 Prozent (Abb. 24). Diese Entwicklung stimmt nachdenklich, denn der Umgang mit e-Crime-Angriffen sollte nicht ausschließlich im Parallelbetrieb zur täglichen Arbeit in der IT-Abteilung erfolgen, sondern erfordert Mitarbeiter mit spezifischeren Kenntnissen und einem stetigen Fokus auf e-Crime. Ursächlich für die vermehrte Nennung der Abteilung könnte jedoch ebenso sein, dass viele Unternehmen zwar durchaus über ein Security Operations Center, ein Computer Emergency Response Team oder vergleichbare spezialisierte Einheiten verfügen, dass diese aber organisatorisch der IT-Abteilung unterstellt sind (vgl. Kapitel 4).

Insbesondere große Unternehmen scheinen zunehmend zu erkennen, dass eine stärkere Spezialisierung und Fokussierung auf die Thematik notwendig ist, denn sie nutzen im Vergleich zu kleinen und mittleren Unternehmen (52 beziehungsweise 59 Prozent) zur Aufklärung vermehrt einen eigenen Bereich für IT-Sicherheit (73 Prozent).

Die Compliance- und die Rechtsabteilung (38 beziehungsweise 34 Prozent) spielen im Vergleich zur Studie aus dem Jahr 2017 eine geringere Rolle (2017: 42 gegenüber 36 Prozent). Die Aufklärung durch die Interne Revision rückt sogar noch stärker in den Hintergrund (2017: 41 Prozent; 2019: 31 Prozent).

Im Vergleich zur Studie des Jahres 2017 gewinnen bei der Aufklärung neben der IT-Abteilung die Unternehmenssicherheit, externe IT-Sicherheits- und externe Forensic-Dienstleister an Bedeutung. So betraut nun knapp jeder Dritte (30 Prozent) die Unternehmenssicherheit mit der Aufklärung, etwa jeder Vierte externe IT-Sicherheitsdienstleister und jeder Zehnte externe Forensic-Dienstleister.

Große Unternehmen sind in dieser Hinsicht grundsätzlich breiter aufgestellt. Mindestens die Hälfte von ihnen bezieht regelmäßig sieben der elf abgefragten Einheiten in die Aufklärung von e-Crime-Delikten ein. Kleine und mittlere Unternehmen nehmen hingegen nur die Dienste von zwei der elf abgefragten Optionen in Anspruch.

Dass nur externe IT-Sicherheitsdienstleister mit der operativen Aufklärung beauftragt werden oder die Durchführung im alleinigen Verantwortungsbereich der Geschäftsführung liegt, geben eher kleinere und mittlere Unternehmen an. Der Grund hierfür könnte darin liegen, dass insbesondere kleine Unternehmen schlicht nicht über spezialisierte Abteilungen verfügen, die gezielt für Compliance oder Interne Revision zuständig sind. Die operative Aufklärung allein in den Händen der Geschäftsführung zu lassen, ist besonders riskant, da diese in der Regel nicht über genügend Ressourcen für eine lückenlose Aufklärung verfügt.

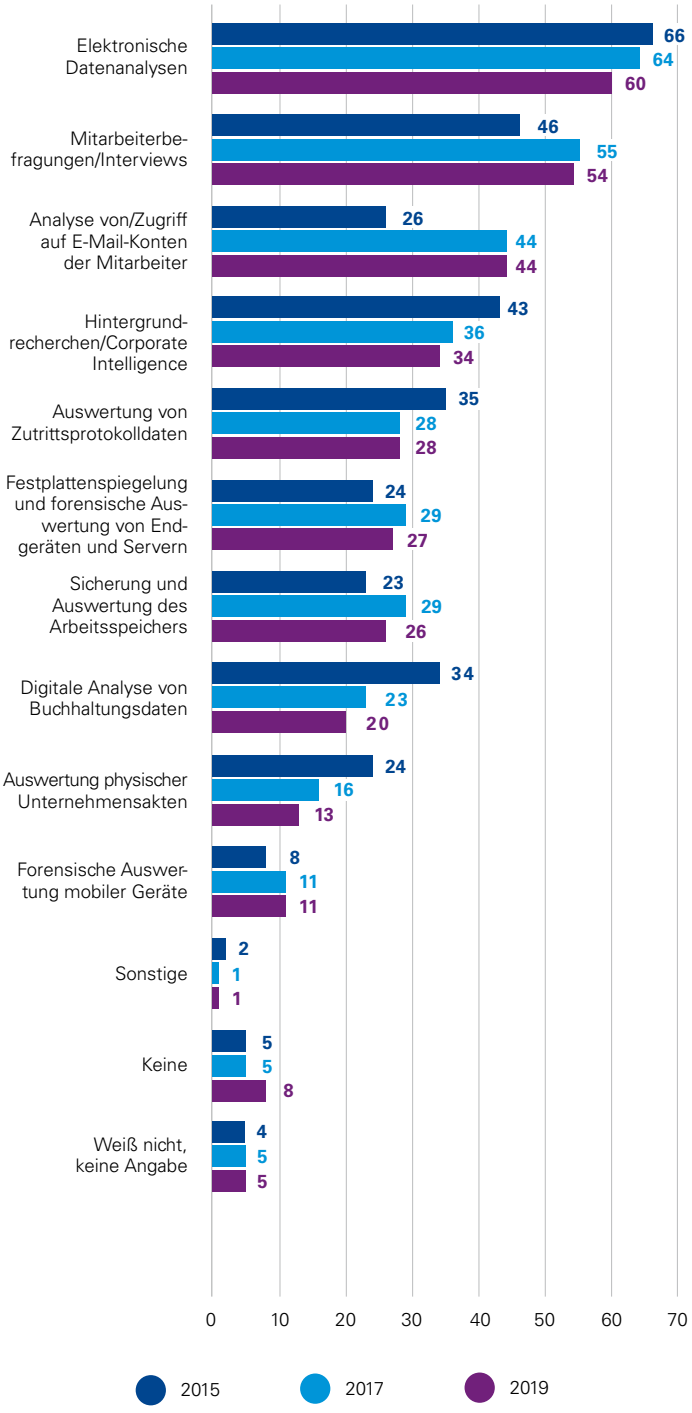
Die streng regulierten Unternehmen der Finanzbranche arbeiten bei der Aufklärung doppelt so häufig mit Strafverfolgungsbehörden zusammen wie Befragte anderer Branchen. Ein ähnliches Bild zeigt sich auch bei der Einbindung der Compliance-Abteilung und der Internen Revision. Meistgenannt ist jedoch die IT-Sicherheitsabteilung mit 70 Prozent.

3.2.3. Maßnahmen zur Aufklärung

Mit Blick auf die zur Aufklärung von e-Crime ergriffenen Maßnahmen sind keine größeren Unterschiede zu den Ergebnissen des Jahres 2017 festzustellen (Abb. 25). Nach wie vor sind elektronische Datenanalysen (60 Prozent) sowie Mitarbeiterbefragungen oder Interviews (54 Prozent) die meistgenannten Aufklärungsmaßnahmen.

Als dritthäufigstes von den betroffenen Unternehmen genutztes Instrument hat sich die Analyse von E-Mail-Konten der Mitarbeiter etabliert (44 Prozent). Angesichts der hohen Betroffenheit von Mailservern ist es bei vielen Delikten erforderlich, E-Mail-Konten von Beschäftigten auszuwerten. Einige Delikte, etwa der Fake-President-Betrug, sind in vielen Fällen ohne die Verwendung von E-Mails kaum zu realisieren, sodass die entsprechenden Postfächer bei der Aufklärung notwendigerweise zu überprüfen sind.

Abb. 25: Aufklärungsmaßnahmen
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Etwas mehr als ein Drittel aller Betroffenen (34 Prozent) führt zudem Hintergrundrecherchen durch. Große Unternehmen (53 Prozent) tun dies wesentlich häufiger als die übrigen (kleine Unternehmen: 34 Prozent; mittlere Unternehmen: 29 Prozent). Es ist davon auszugehen, dass umsatzstarke Unternehmen über eigene, auf Corporate Intelligence spezialisierte Abteilungen verfügen oder externe Stellen mit solchen Recherchen beauftragen.

Jeweils etwas mehr als ein Viertel der Betroffenen nennt zudem die Auswertung von Zutrittsprotokolldaten (28 Prozent), die Festplattenspiegelung und forensische Auswertung von Laptops, Workstations und Servern (27 Prozent) sowie die Sicherung und Auswertung des Arbeitsspeichers (26 Prozent).

Überraschend ist, dass immerhin 8 Prozent der betroffenen Unternehmen angeben, keinerlei Maßnahmen zur Aufklärung ergriffen zu haben, wobei dies insbesondere auf kleine Unternehmen zutrifft (11 Prozent). Möglicherweise betreiben Betroffene bei Vorfällen mit geringen Schadenssummen keine weiteren Anstrengungen zur Aufklärung, da die damit verbundenen Kosten aus ihrer Sicht den Aufwand nicht rechtfertigen. Damit lassen sich Unternehmen allerdings die Chance entgehen, die Schwachstellen und Fehler, die den e-Crime-Vorfall ermöglicht haben, zu identifizieren und zu korrigieren.

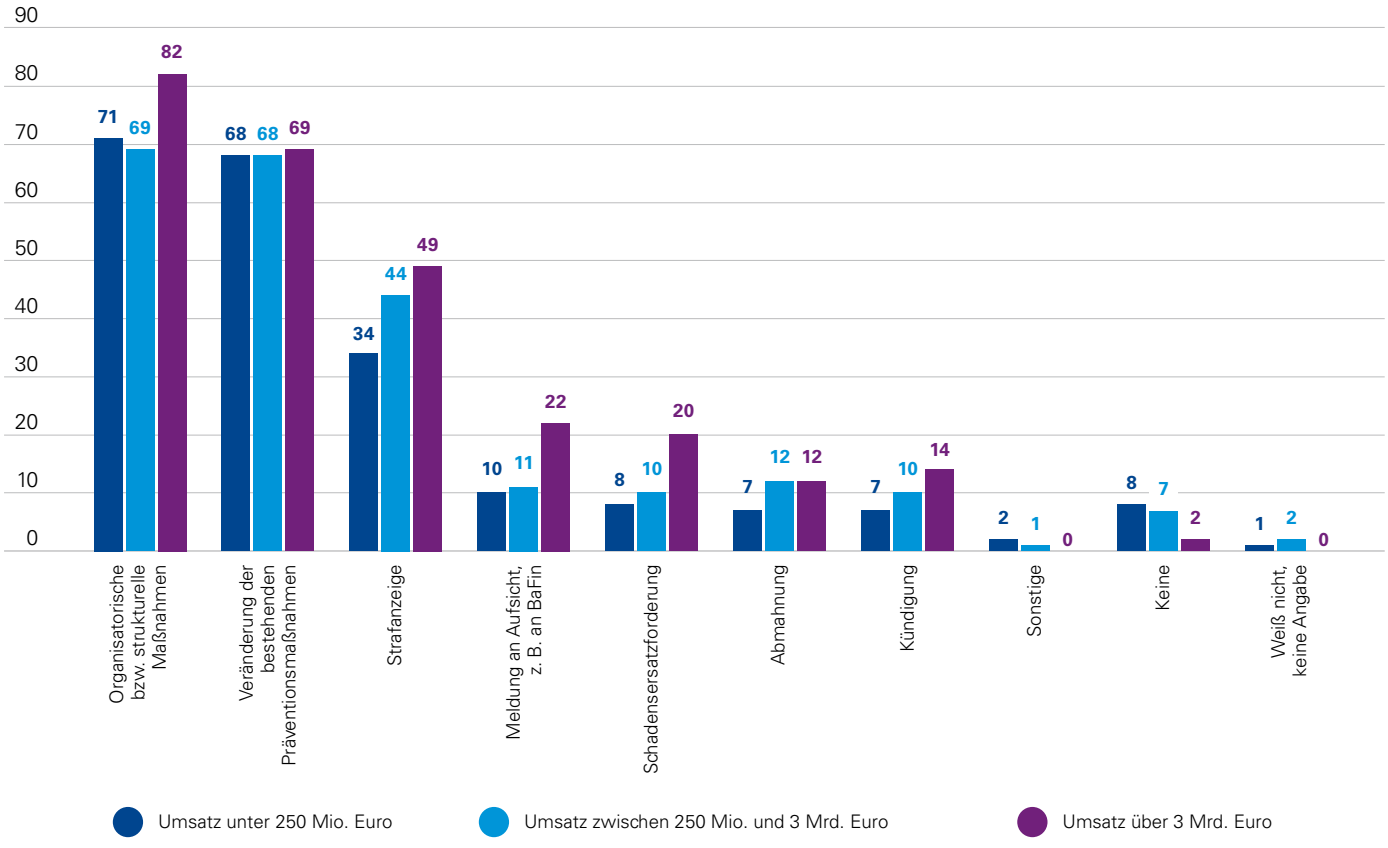
3.3. Reaktion und Sanktionierung

3.3.1. Maßnahmen nach der Aufklärung

Als Reaktion auf e-Crime-Vorfälle ergreifen die meisten Unternehmen organisatorische oder strukturelle Maßnahmen (72 Prozent). In Betracht kommen beispielsweise die Neuzuordnung von Verantwortlichkeiten und die Einrichtung eines SOC oder CERT.

Gut zwei Drittel der Befragten (68 Prozent) haben infolge eines Vorfalls ihre Präventionsmaßnahmen angepasst (Abb. 26). Dies ist gerade im Feld der Computerkriminalität ein bedeutsamer Schritt, da neuartige Technologien stets eine Überarbeitung der bereits getroffenen Maßnahmen erfordern und Unternehmen sich stetig gegen neue Angriffsmuster wappnen müssen.

Abb. 26: Maßnahmen nach Vorfall
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Zwei von fünf Betroffenen haben Strafanzeige erstattet. Hierbei gilt es zu berücksichtigen, dass 85 Prozent der Täter lediglich als unbekannte Externe klassifiziert werden können. Dementsprechend wird es für Unternehmen in vielen Fällen schwierig sein, eine hinreichend konkrete Anzeige zu erstatten.

Die weiteren abgefragten Maßnahmen – Meldung an die zuständige Aufsichtsbehörde (12 Prozent), Schadensersatzforderungen (10 Prozent), Abmahnungen (10 Prozent) und Kündigungen (9 Prozent) – wurden jeweils von circa einem von zehn Betroffenen angegeben.

Umsatzstärkere Unternehmen ergreifen nach Vorfällen eine größere Bandbreite an Maßnahmen. Dies zeigt sich insbesondere bei organisatorischen und strukturellen Maßnahmen (82 Prozent), Strafanzeigen (49 Prozent), Meldungen an die Aufsichtsbehörden (22 Prozent) und Schadensersatzforderungen (20 Prozent). Sie setzen das Mehr an verfügbaren Ressourcen in der Reaktion somit gezielt ein. Hinzu kommt, dass die Meldung an die zuständigen Behörden vor allem im stark regulierten Finanzsektor genannt wird (35 Prozent), der wiederum einen hohen Anteil umsatzstarker Unternehmen stellt.

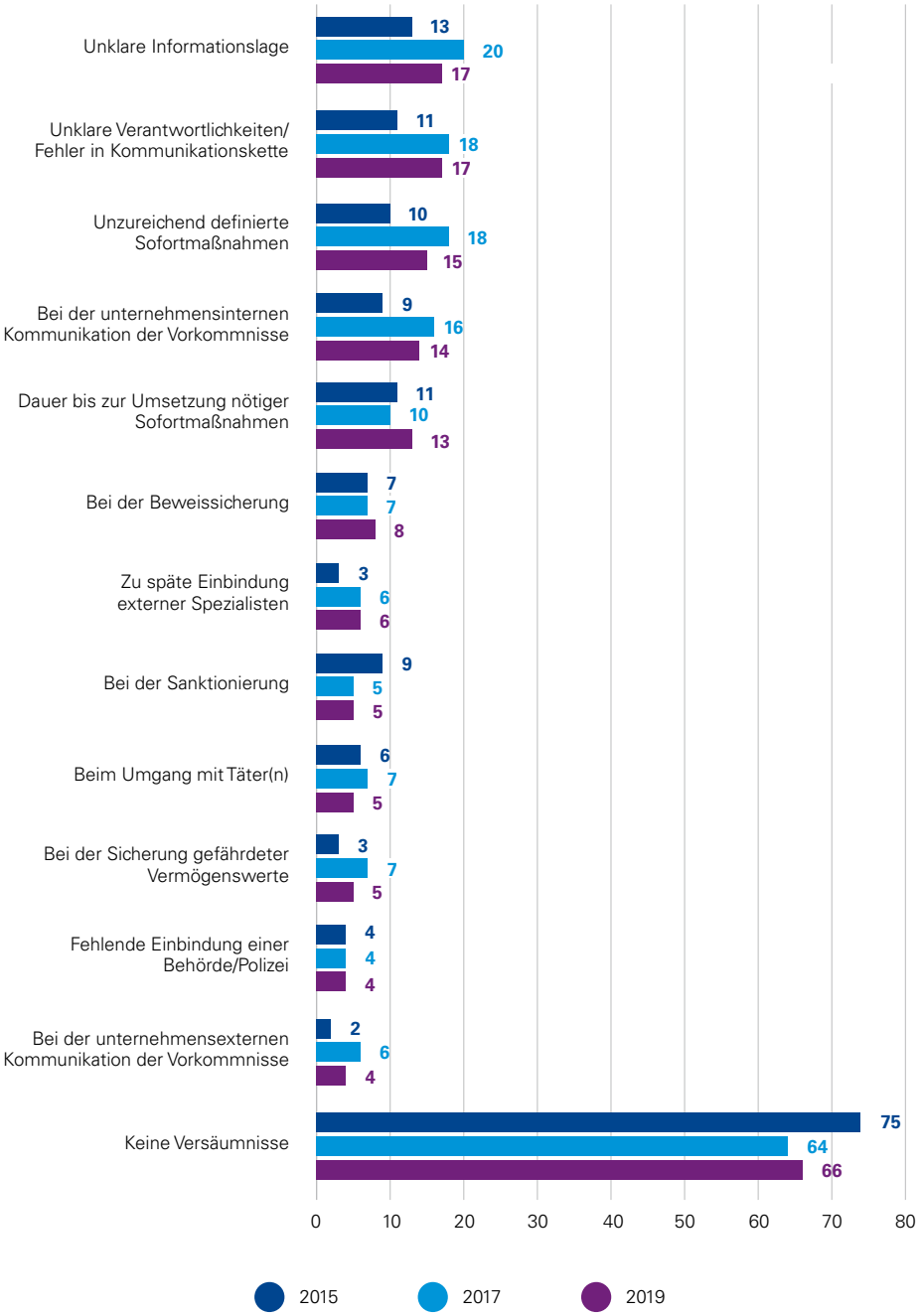
Immerhin 7 Prozent der Betroffenen haben infolge eines e-Crime-Vorfalls keine weiteren Maßnahmen ergriffen. Dies birgt große Risiken: Zum einen werden potenzielle (Innen-)Täter nicht durch eine entsprechende Sanktionierung abgeschreckt – so verweisen tatsächlich drei Viertel der Befragten auf die Annahme der Täter, straffrei zu bleiben, als e-Crime-begünstigenden Faktor. Zum anderen bleiben bei einer derartigen Untätigkeit Schwachstellen unverändert bestehen.

3.3.2. Versäumnisse bei der Reaktion

Nahezu unverändert im Vergleich zur Studie des Jahres 2017 gibt ein Drittel (34 Prozent) der Betroffenen an, im eigenen Unternehmen Versäumnisse im Umgang mit e-Crime zu sehen. Der positive Trend eines zunehmend selbstkritischen Blicks auf die eigene Reaktion ist somit zunächst gestoppt (2015: 25 Prozent).

Nach wie vor bereiten den Unternehmen insbesondere die Kommunikation und die unmittelbare Vorfallsbehandlung Schwierigkeiten, vor allem bei der Erstreaktion. So nimmt mehr als jedes sechste Unternehmen Versäumnisse in Bezug auf eine unklare Informationslage wahr (17 Prozent). Selbiges gilt für den Aspekt unklarer Verantwortlichkeiten und das Auftreten von Fehlern in der Kommunikationskette (Abb. 27). Darüber hinaus sieht jeder siebte Betroffene Schwierigkeiten bei der unternehmensinternen Kommunikation bezüglich der Vorkommnisse (14 Prozent). Dass Unternehmen vor allem in dieser Hinsicht Versäumnisse erkennen, zeigt, dass sie sich des Stellenwerts einer präzisen und geradlinigen Kommunikation beim Umgang mit e-Crime durchaus bewusst sind. Um einen für die Aufklärung essentiellen schnellen, zielgerichteten Informationsfluss zu gewährleisten, bietet es sich an, Krisenreaktions- und Kommunikationspläne festzulegen, die Verantwortlichkeiten zuordnen und Kommunikationswege vorgeben. Davon profitiert die Erstreaktion erheblich, die zur Eindämmung von Auswirkungen und Schäden maßgeblich ist.

Abb. 27: Versäumnisse
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Versäumnisse räumen die Betroffenen auch bei ihren Sofortmaßnahmen ein, einem weiteren wichtigen Bestandteil der Erstreaktion. So geben 15 Prozent der Unternehmen an, dass Sofortmaßnahmen unzureichend definiert seien, weitere 13 Prozent betrachten die Dauer bis zu ihrer Umsetzung kritisch. Auch in dieser Hinsicht ist die Wirkung eines zuvor ausgearbeiteten Maßnahmenkonzepts nicht zu unterschätzen. Es muss sichergestellt werden, dass bestimmte Schritte (beispielsweise die korrekte, gegebenenfalls forensische Sicherung von Daten) bei jedem Vorfall eingehalten werden. Allerdings muss bei diesen Konzepten eine gewisse Flexibilität gewahrt werden, damit Lösungen in einem angemessenen Zeitrahmen angepasst werden können. Die Annahme, alle Vorfälle auf eine einheitliche Art und Weise bearbeiten zu können, wäre ein Trugschluss.

Wie in der Studie des Jahres 2017 sehen vor allem Befragte mittelgroßer Unternehmen verhältnismäßig wenige Versäumnisse (25 Prozent), verglichen mit Vertretern der anderen Kategorien (klein: 38 Prozent; groß: 47 Prozent). Gerade bei großen Unternehmen geht dies damit einher, dass die Befragten nicht nur grundsätzlich häufiger Versäumnisse konstatieren, sondern diese auch wesentlich vielschichtiger wahrnehmen. So werden zehn der zwölf abgefragten Aspekte zumindest von einem Zehntel der großen Unternehmen genannt. Bei mittleren Unternehmen sind es lediglich drei Antwortmöglichkeiten. Dies könnte darauf zurückzuführen sein, dass große Unternehmen sich angesichts einer höheren festgestellten Betroffenheit schlichtweg mit mehr Fällen auseinandersetzen müssen und dementsprechend mehr Versäumnisse feststellen können. Auch große Unternehmen machen als Defizite insbesondere Folgendes aus: unklare Informationslage (33 Prozent), unklare Verantwortlichkeiten (33 Prozent) und unzureichend definierte Sofortmaßnahmen (27 Prozent).

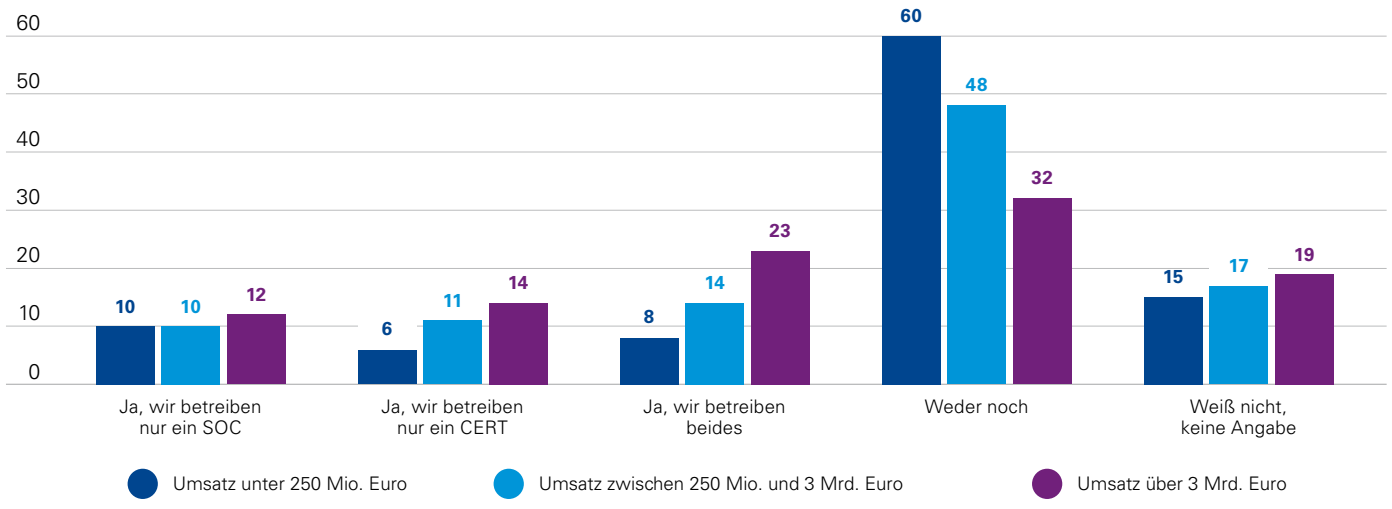
Sicherheit mit System

04 SOC/CERT

Der Schutz der IT-Infrastruktur wie auch der Unternehmensdaten vor internen und externen Gefahren hat sich in den vergangenen Jahren immer weiter professionalisiert. Beispiele dafür sind Security Operations Center (SOC) sowie Computer Emergency Response Teams (CERT), mit denen die Unternehmen den zunehmend komplexen e-Crime-Delikten entgegentreten. Bei einem SOC handelt es sich um eine zentrale Stelle, die alle sicherheitsrelevanten Unternehmenssysteme und -prozesse in Echtzeit überwacht. Dadurch können Bedrohungen sofort erkannt und Gegenmaßnahmen eingeleitet werden. Ein CERT hingegen leistet zum einen präventive Arbeit durch die Identifizierung von Sicherheitslücken, zum anderen ergreift es Abwehrmaßnahmen bei konkreten Vorfällen. Grundsätzlich können SOC und CERT dazu beitragen, die Bekämpfung von e-Crime zu strukturieren und zu professionalisieren. Eine derartige klare Organisationsstruktur, die Zuständigkeiten und Notfallpläne beinhaltet, ist beim Umgang mit Computerkriminalität von unschätzbarem Wert.

Jeweils rund ein Fünftel der Unternehmen, die an der Studie teilgenommen haben, betreibt ein SOC (22 Prozent) oder ein CERT (21 Prozent). Über beide Einheiten zugleich verfügen sogar 12 Prozent der Befragten (Abb. 28).

Abb. 28: Vorhandensein SOC/CERT nach Unternehmensgröße
Angaben in Prozent



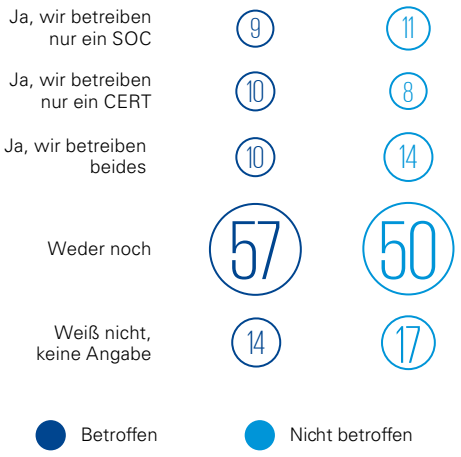
Quelle: KPMG in Deutschland, 2019

Besonders bemerkenswert ist, dass Unternehmen, die bislang nicht von e-Crime betroffen waren, besser als die übrigen Befragten ausgestattet sind, was SOC und CERT anbelangt (Abb. 29). Dies könnte ein Indiz für die präventive Wirkung dieser Einheiten sein. Allerdings beugen sie e-Crime nicht nur vor, sondern tragen auch dazu bei, Vorfälle rasch aufzudecken, sodass unverzüglich angemessene Maßnahmen zur Abwehr und Schadensminimierung ergriffen werden können. Unterstrichen wird dies dadurch, dass etwa vier von fünf nicht betroffenen Unternehmen zudem einen Incident Response-Prozess implementiert haben, der sie prozessual und organisatorisch in die Lage versetzt, adäquat, effektiv und kurzfristig auf Sicherheitsvorfälle zu reagieren. Bei Betroffenen trifft dies lediglich auf etwas mehr als zwei Drittel zu.

Betrachtet man die Ergebnisse nach Umsatzklassen, zeigt sich, dass größere Unternehmen häufiger als andere mindestens eine der beiden Optionen nutzen. Über beide Einheiten verfügt fast jedes vierte große Unternehmen (23 Prozent), bei den mittleren gilt dies nur für 14 Prozent und bei den kleinen sogar nur für 8 Prozent. Als Ursache könnte infrage kommen, dass kleine und mittlere Unternehmen nicht über die notwendigen finanziellen Ressourcen für die Einrichtung von SOC oder CERT verfügen. Denkbar ist allerdings auch, dass sie sich noch nicht ausreichend mit derartigen Einheiten auseinandergesetzt haben und sie daher nicht in Betracht ziehen.

Größere Unternehmen beschäftigen mehr Personen in den jeweiligen Teams als kleinere. So besteht bei jedem dritten

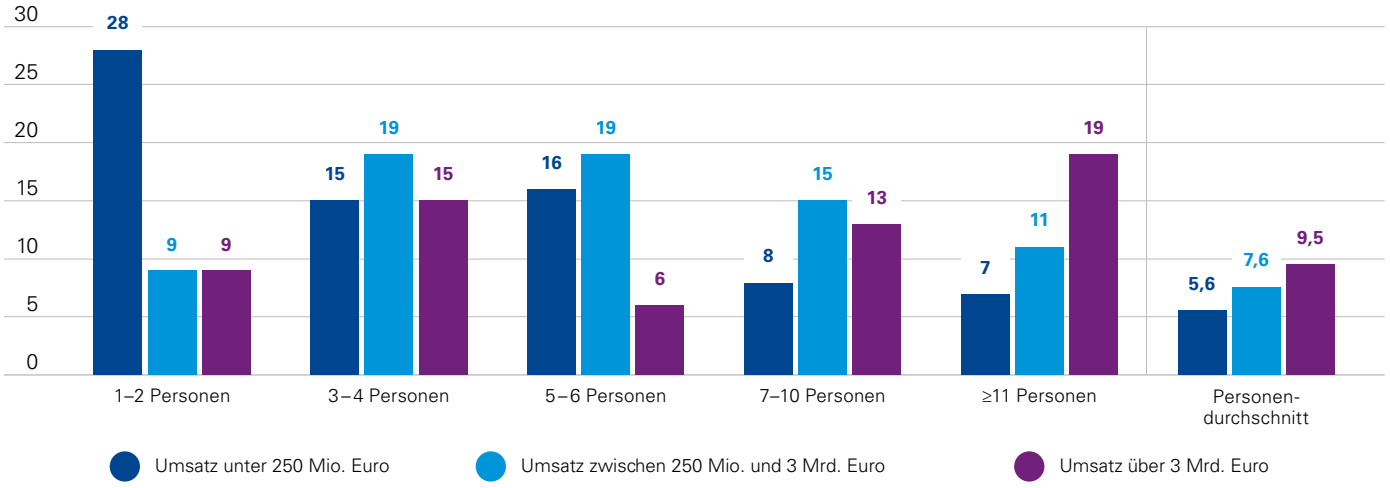
Abb. 29: Vorhandensein SOC/CERT bei betroffenen bzw. nicht betroffenen Unternehmen
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

großen Unternehmen das SOC oder CERT aus mehr als sieben Mitarbeitern; dies trifft jedoch nur auf jedes vierte mittlere und nur auf jedes sechste kleine Unternehmen (Abb. 30) zu. Des Weiteren fällt auf, dass diese Einheiten in Unternehmen, die bisher nicht von Computerkriminalität betroffen waren, im Durchschnitt mit acht Personen besetzt sind, bei den übrigen Befragten jedoch nur mit 5,7. Dies deutet an, dass die Effektivität von SOC und CERT nicht zuletzt von ihrer personellen Ausstattung abhängt.

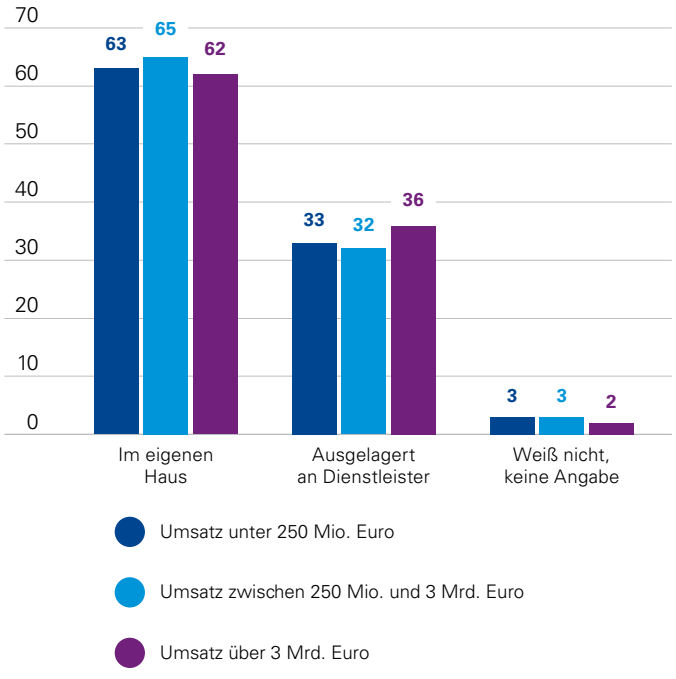
Abb. 30: Anzahl der SOC-/CERT-Beschäftigten
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

SOC wie auch CERT werden über alle Umsatzklassen hinweg von knapp zwei Dritteln der Unternehmen im eigenen Haus betrieben (Abb. 31), wohingegen etwa ein Drittel diese Funktionen an externe Dienstleister auslagert. Die einzige Ausnahme bilden Finanzdienstleister, bei denen in 51 Prozent der Fälle Externe für den Betrieb zuständig sind. Das könnte daher rühren, dass Finanzunternehmen grundsätzlich in einem höheren Maße IT an externe Dienstleister auslagern als Unternehmen anderer Branchen. Dies zeigt sich auch mit Blick auf die von e-Crime tatsächlich betroffenen IT-Bereiche.

Abb. 31: Interner oder externer Betrieb
Angaben in Prozent

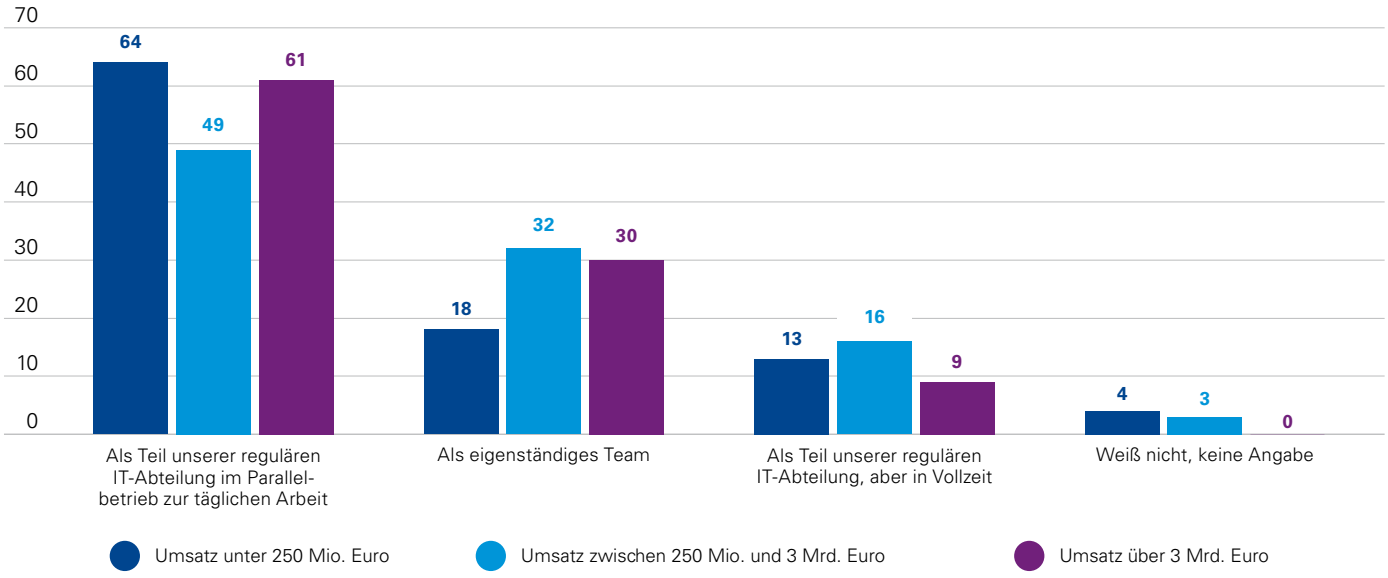


Quelle: KPMG in Deutschland, 2019

Bei etwas mehr als jedem vierten Unternehmen, das ein SOC oder CERT im eigenen Haus betreibt, stellen diese Einheiten ein eigenständiges Team dar. Der Großteil der Unternehmen allerdings (57 Prozent) sieht das eigene SOC und CERT als Teil der regulären IT-Abteilung im Parallelbetrieb zur täglichen Arbeit. Nur etwa jedes siebte Unternehmen hat für das SOC oder CERT Vollzeitstellen geschaffen, die an die reguläre IT angegliedert sind.

Unterschiede zeigen sich insbesondere bei den Umsatzklassen. Knapp ein Drittel der mittleren und großen Unternehmen organisieren SOC oder CERT als eigenständiges Team (Abb. 32). Dies trifft jedoch nur auf 18 Prozent der kleinen Unternehmen zu, die diese Einheiten meist in der IT im Parallelbetrieb unterhalten (64 Prozent). Auch große Unternehmen gehen zu 61 Prozent diesen Weg. Fraglich ist hier, ob die Effektivität eines SOC oder CERT leidet, wenn es parallel neben der regulären IT betrieben wird. Unter Umständen könnte die Einrichtung weiterer eigenständiger Vollzeitstellen mit ausschließlicher Zuständigkeit für Prävention, ständiges Systemmonitoring und Erstellung angemessener Notfallpläne sowie zur Reaktion auf konkrete Cyber-Vorfälle dazu beitragen, dass diese Einheiten ihre Aufgaben noch besser erfüllen.

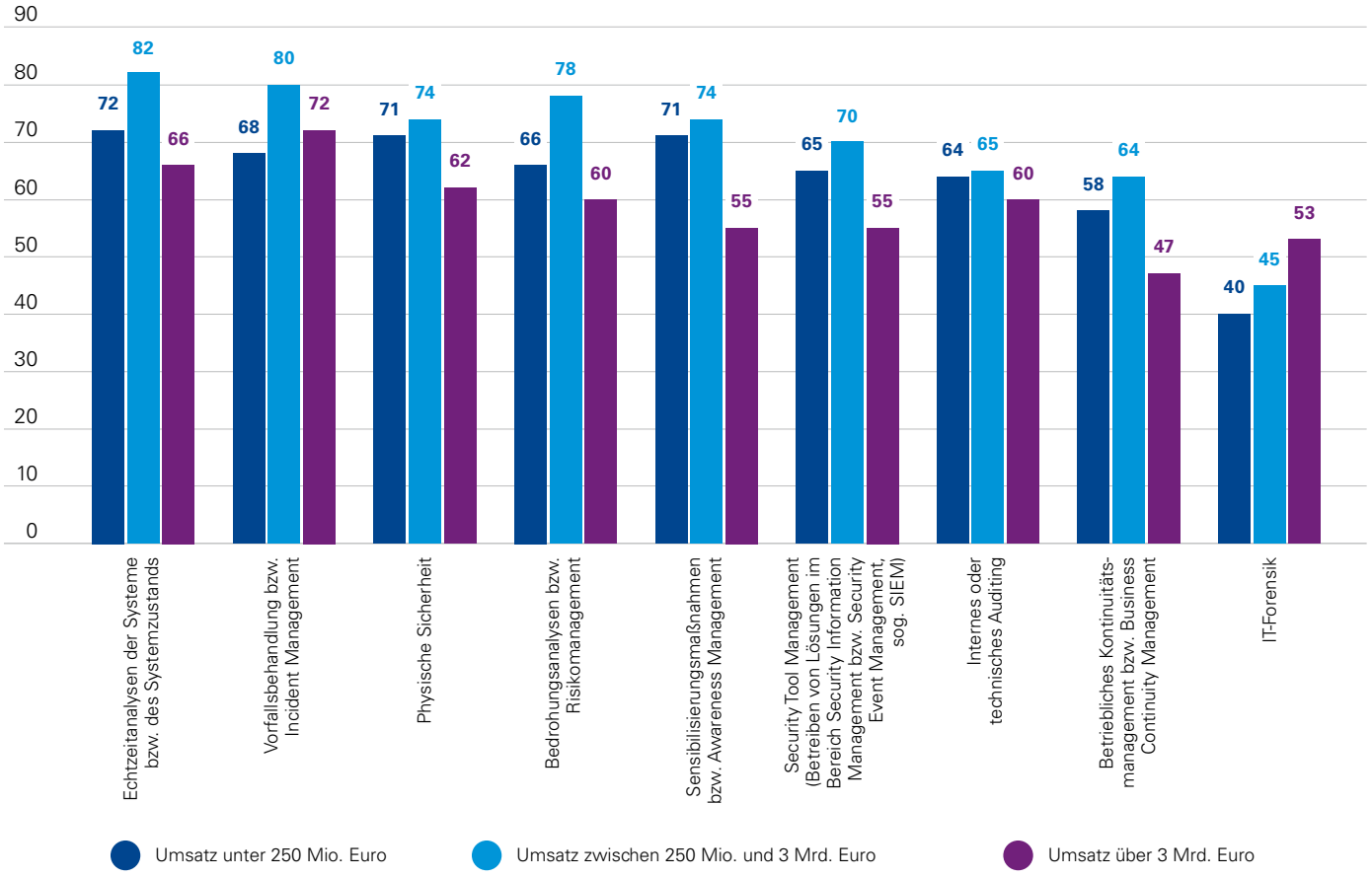
Abb. 32: Betrieb SOC/CERT
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Zumeist ist es die Aufgabe von SOC oder CERT, Systeme und Systemzustand in Echtzeit zu analysieren und im Rahmen des Incident Managements Vorfälle gezielt zu behandeln. Beide Aufgabenbereiche werden jeweils von knapp drei Vierteln der Befragten genannt. In der Regel sind Unternehmen jedoch breiter aufgestellt, denn rund zwei Drittel aller Befragten zählen auch die physische Sicherheit (71 Prozent), Bedrohungsanalysen (70 Prozent), Sensibilisierungsmaßnahmen (70 Prozent), Security Tool Management (65 Prozent) sowie internes oder technisches Auditing zu den Aufgabenbereichen des SOC oder CERT. Ein betriebliches Kontinuitätsmanagement (59 Prozent) sowie die IT-Forensik (44 Prozent) werden hingegen deutlich seltener genannt.

Abb. 33: Aufgabenbereiche SOC/CERT
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

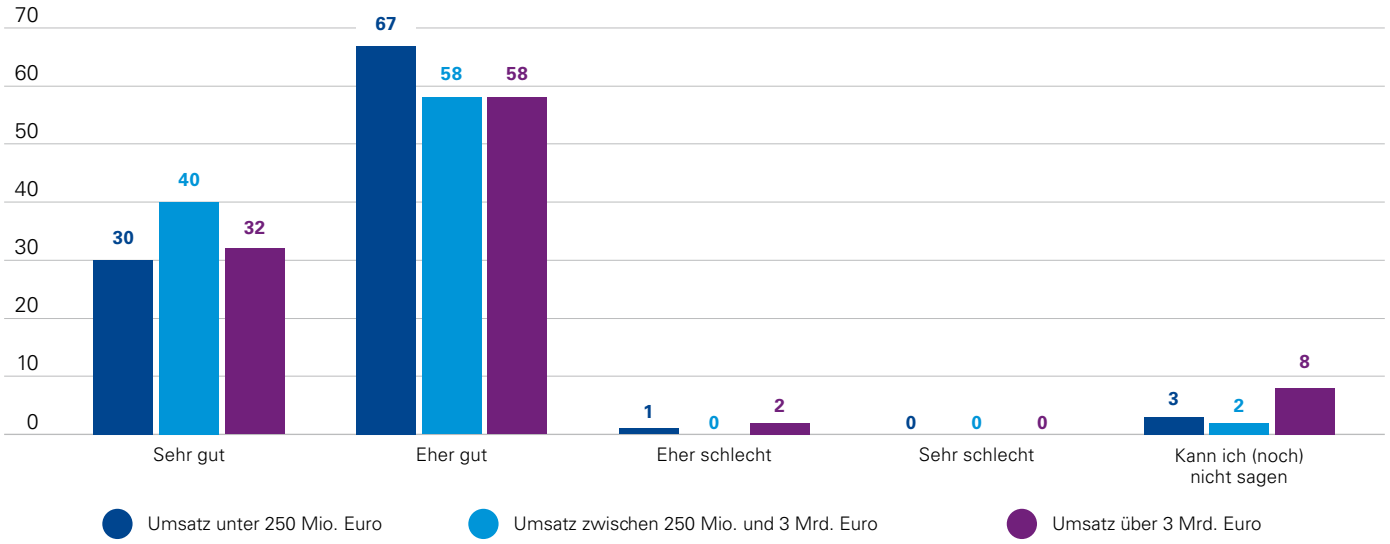
Überraschend ist, dass mehr als ein Drittel der Unternehmen im SOC oder CERT kein Security Tool Management integriert hat, sprich das Betreiben von Lösungen im Bereich Security Information beziehungsweise Security Event Management (SIEM). Derartige Maßnahmen sollten allerdings mittlerweile Standard in der deutschen Wirtschaft sein.

Auffällig ist, dass mittelgroße Unternehmen nahezu alle Aufgabenbereiche prozentual häufiger in ihrem SOC oder CERT verorten als kleine und große (Abb. 33). Die einzige Ausnahme bildet die IT-Forensik, die gut jedes zweite große Unternehmen als SOC- oder CERT-Bestandteil ausweist, was bei mittleren und kleinen Unternehmen seltener der Fall ist (45 beziehungsweise 40 Prozent).

Von Computerkriminalität nicht betroffene Unternehmen verfügen in ihrem SOC oder CERT im Mittel häufiger über sämtliche abgefragten Disziplinen als bereits betroffene Unternehmen. Dies spricht erneut für die Effektivität dieser Einheiten. Ihre Einführung ist daher von unschätzbarem Wert für die Prävention von e-Crime und den Umgang mit Angriffen im Ernstfall.

Die Wirksamkeit des eigenen SOC oder CERT schätzt ein Drittel aller Befragten als sehr gut ein, die meisten weiteren Befragten bewerten es als eher gut und nur 1 Prozent der Unternehmen als eher schlecht (Abb. 34). Im Vergleich nach Umsatzklassen beurteilen vor allem mittlere Unternehmen die Wirksamkeit dieser Einrichtungen besonders gut: Vier von zehn wählen die Antwortmöglichkeit „sehr gut“. Dies trifft nur auf etwa drei von zehn der übrigen Befragten zu. Die Ursache könnte darin zu finden sein, dass Unternehmen dieser Kategorie die abgefragten Aufgabenbereiche tatsächlich häufiger umsetzen, was die Angaben bei der Frage nach den im SOC oder CERT verorteten Disziplinen nahelegen.

Abb. 34: Einschätzung Wirksamkeit
Angaben in Prozent

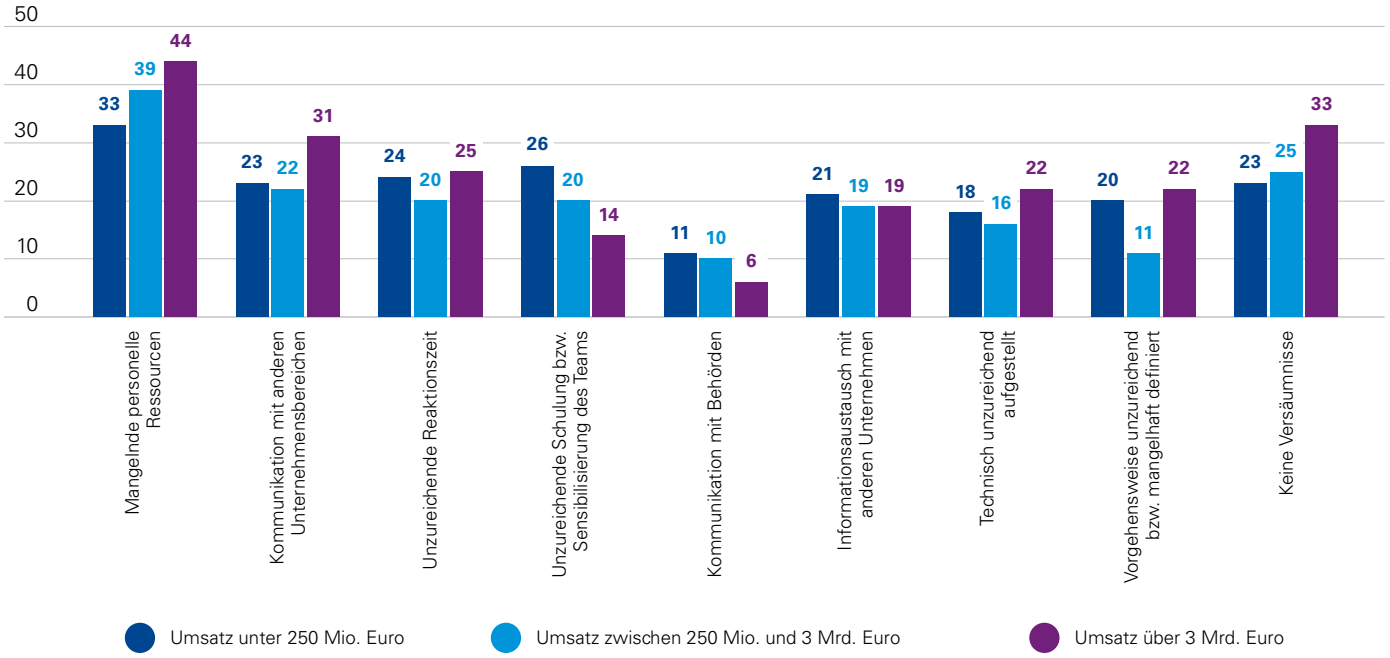


Quelle: KPMG in Deutschland, 2019

Obwohl 96 Prozent der Unternehmen die Wirksamkeit des SOC oder CERT mindestens als eher gut einschätzen, sehen etwa drei Viertel von ihnen in diesem Bereich auch Versäumnisse (Abb. 35). Dabei fällt auf, dass bereits von e-Crime betroffene Unternehmen seltener Versäumnisse im Zusammenhang mit ihrem SOC oder CERT sehen als nicht betroffene Unternehmen: Ein Drittel von ihnen gibt keine zu Protokoll, wohingegen dies nur für etwa ein Fünftel der nicht Betroffenen gilt. Die Ergebnisse dieser Studie rechtfertigen diese Selbsteinschätzung allerdings nicht – ganz im Gegenteil: Sie belegen, dass nicht betroffene Unternehmen hinsichtlich der im SOC oder CERT vereinten Disziplinen über einen deutlichen Vorsprung vor den Betroffenen verfügen.

Zumeist sehen die befragten Unternehmen Versäumnisse im SOC oder CERT aufgrund mangelnder personeller Ressourcen (37 Prozent). Darüber hinaus stellen die Kommunikation mit anderen Unternehmensbereichen (24 Prozent) und eine unzureichende Reaktionszeit (23 Prozent) etwa jedes vierte Unternehmen vor Probleme. Etwa jeder Fünfte gibt an, die Wirksamkeit von SOC oder CERT werde durch unzureichende Schulung beziehungsweise Sensibilisierung des Teams (22 Prozent), einen mangelnden Informationsaustausch mit anderen Unternehmen (20 Prozent), eine nicht ausreichende technische Ausstattung sowie eine unzureichend definierte Vorgehensweise (17 Prozent) beeinträchtigt. Versäumnisse bei der Kommunikation mit Behörden sieht nur ein kleiner Anteil der Unternehmen (9 Prozent).

Abb. 35: Versäumnisse in der Wirksamkeit von SOC oder CERT
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Ein Drittel der großen Unternehmen gibt an, keine Versäumnisse wahrzunehmen, ebenso wenig jedes vierte der kleinen und mittleren Unternehmen. Paradoxerweise sehen Vertreter großer Unternehmen mit Blick auf fünf der acht abgefragten Einzelaspekte jedoch größere Schwierigkeiten als die übrigen Studienteilnehmer. Insbesondere ist überraschend, dass sie häufiger mangelnde personelle Ressourcen (44 Prozent) und eine unzureichende technische Aufstellung (22 Prozent) als die kleinen (33 und 18 Prozent) und mittleren Unternehmen (39 und 16 Prozent) anmerken. Schließlich sind dies grundlegende Faktoren, von denen anzunehmen ist, dass große Unternehmen diese besser beherrschen als kleine. Dies kann darauf hindeuten, dass große Unternehmen im Umgang mit SOC oder CERT bereits routinierter sind und somit ein besseres Verständnis der Aufgaben haben, sodass sie ihre Verbesserungspotenziale gezielter identifizieren können.

Je kleiner ein Unternehmen, desto eher benennt es Schwierigkeiten im Bereich der Schulung und Sensibilisierung der SOC- und CERT-Mitarbeiter. So merkt dies etwa jedes vierte kleine Unternehmen an, jedoch nur circa jedes sechste große. Versäumnisse in diesem Bereich sollten jedoch in jedem Unternehmen – ungeachtet der Größe – schnellstmöglich ausgeräumt werden, da insbesondere der Faktor Mensch einer der Türöffner für Computerkriminalität ist (vgl. Abschnitt 2.6.) und da eine regelmäßige und umfassende Sensibilisierung der Mitarbeiter einen großen Mehrwert in der Prävention bietet.

Vorbereitet für den Ernstfall

05 Cyber-Versicherungen

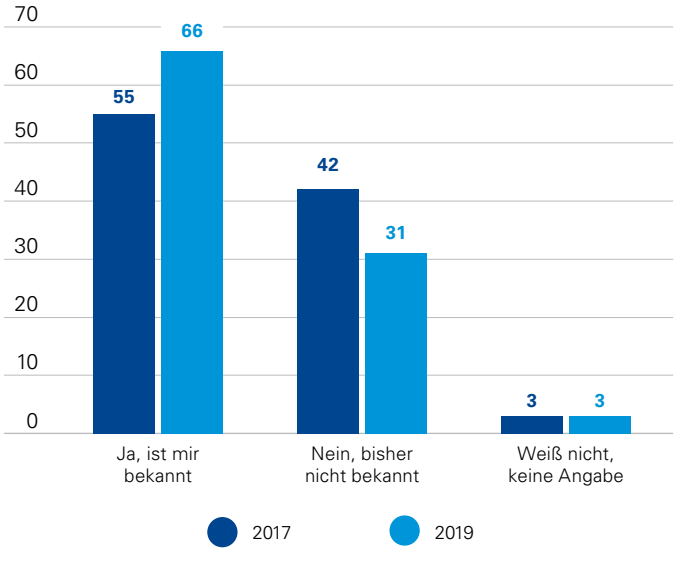
Bereits die e-Crime-Studie des Jahres 2017 befasste sich mit dem Thema Cyber-Versicherungen. Eine solche Versicherung deckt Schäden ab, die durch Computerkriminalität entstehen – je nach Police geschieht dies in unterschiedlicher Breite und Tiefe. Die Ergebnisse der diesjährigen Befragung zeigen, dass das Thema zunehmend im Bewusstsein der Befragten angekommen ist.

Der Anteil der Unternehmen, die um die Möglichkeit wissen, eine Cyber-Versicherung abzuschließen, ist im Vergleich zur vorigen Studie um 20 Prozent gestiegen (Abb. 36). War sich 2017 lediglich etwas mehr als die Hälfte der Befragten dieser Möglichkeit bewusst, sind es nun bereits zwei Drittel.

Darüber hinaus hat von allen Unternehmen, denen die Möglichkeit bekannt war, bereits mehr als ein Viertel eine Cyber-Versicherung abgeschlossen (Abb. 37). Mit Blick auf die Gesamtheit der Studienteilnehmer entspricht dies einer Abdeckung von 18 Prozent. Zudem prüfen weitere 28 Prozent der mit dem Thema vertrauten Unternehmen einen Abschluss. Die Nachfrage nach Cyber-Versicherungen wächst somit. Erwartungsgemäß sind mit einer Abdeckungsrate von fast einem Drittel bis dato insbesondere größere Unternehmen entsprechend versichert.

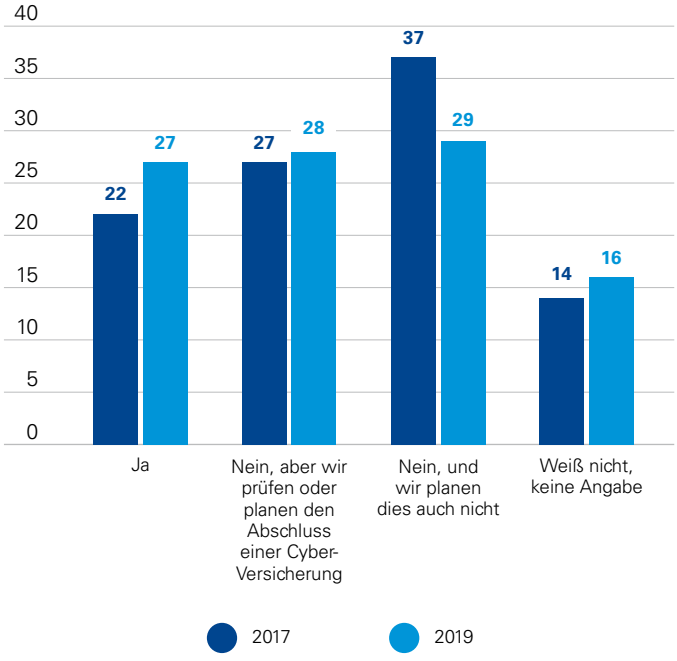
Ferner gab in der jüngsten Befragung kein Unternehmen an, eine Cyber-Versicherung abgeschlossen, aber bereits wieder gekündigt zu haben.

Abb. 36: Bekanntheit Cyber-Versicherung
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Abb. 37: Bestehen einer Cyber-Versicherung
Angaben in Prozent



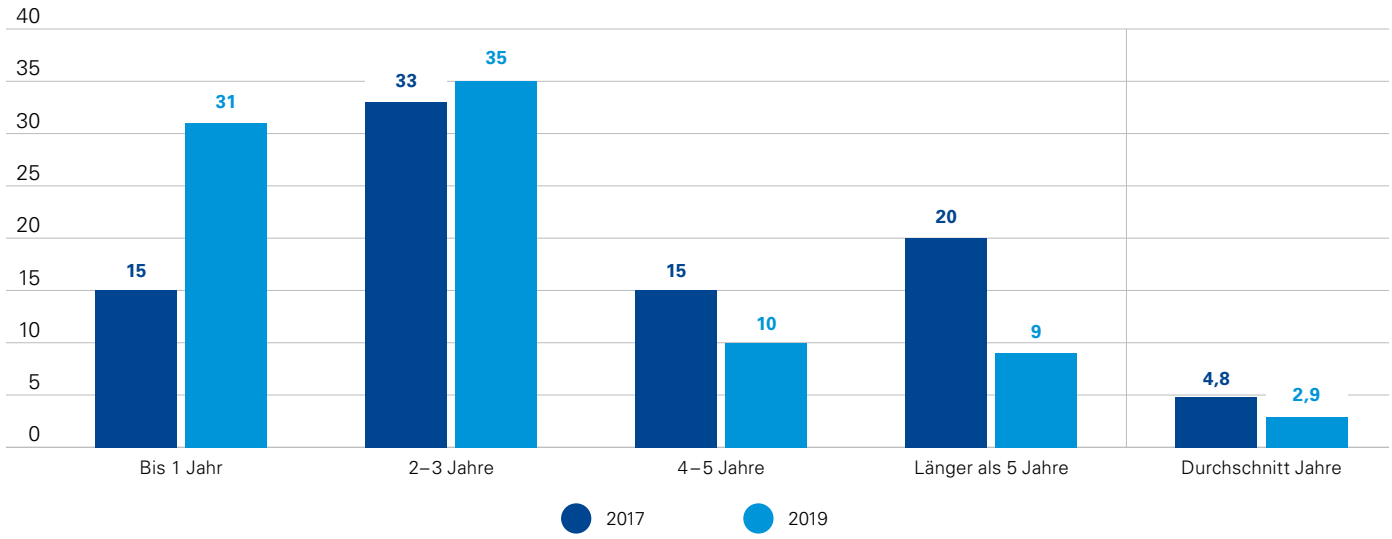
Quelle: KPMG in Deutschland, 2019

Der Anteil der Unternehmen, die in den vergangenen drei Jahren eine entsprechende Versicherung abgeschlossen haben, ist von 48 Prozent im Jahr 2017 auf derzeit 66 Prozent gestiegen (Abb. 38). Dies zeigt einerseits, dass der Markt der Versicherungspolicen noch jung ist, und andererseits, dass diese Versicherungen zunehmend gefragt sind.

Insbesondere bereits betroffene Unternehmen entschieden sich in den beiden zurückliegenden Jahren für den zusätzlichen Schutz einer Cyber-Versicherung (38 Prozent; nicht Betroffene: 25 Prozent). Finanzdienstleister und umsatzstarke Unternehmen verfügen bereits deutlich länger über eine derartige Police: In beiden Kategorien geben mehr als 20 Prozent an, ihre Versicherung bestehe mittlerweile länger als fünf Jahre (21 beziehungsweise 23 Prozent).

Der jeweils größte Anteil der kleinen und mittleren Unternehmen (39 und 35 Prozent) gibt an, den Abschluss einer Cyber-Versicherung zu prüfen oder zu planen. Bei Unternehmen dieser Größenordnungen, die bereits über eine solche verfügen, laufen diese Policen verhältnismäßig oft erst seit drei Jahren.

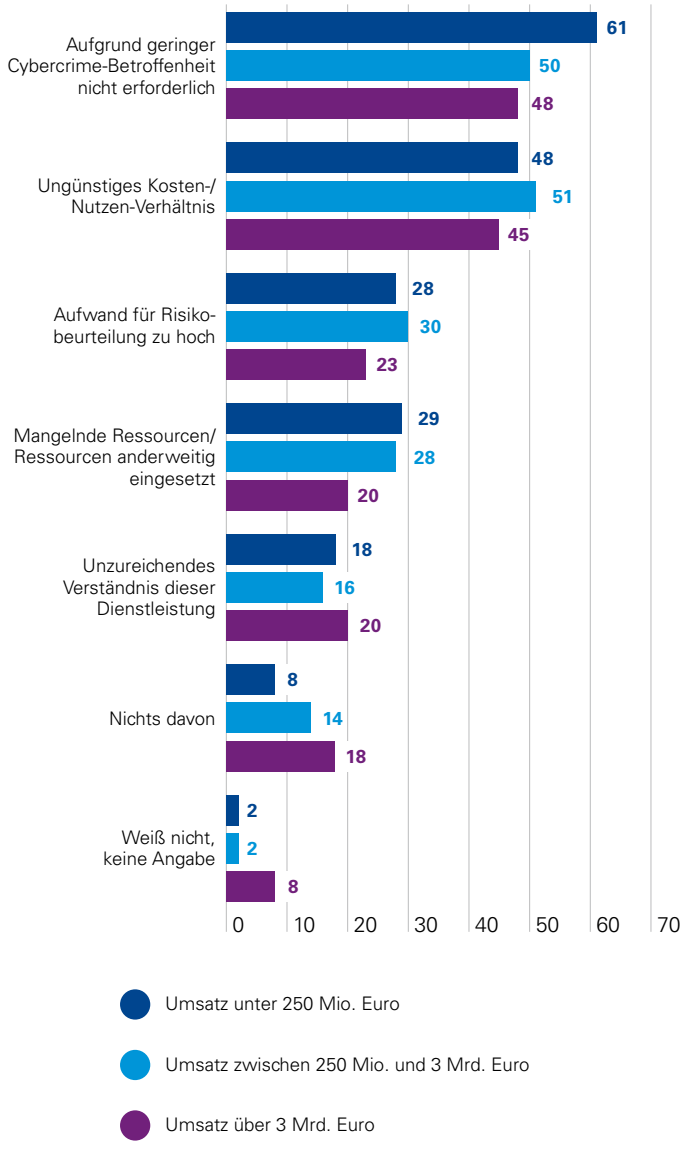
Abb. 38: Dauer des Bestehens einer Cyber-Versicherung
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Nach den Gründen gefragt, wieso Unternehmen noch keine Versicherung abgeschlossen haben, gibt gut die Hälfte der Befragten (55 Prozent) an, dies sei nicht erforderlich, da sie kaum von Computerkriminalität betroffen seien (Abb. 39). Insbesondere wird diese Meinung von kleinen Unternehmen vertreten (61 Prozent). Dies kann jedoch einen gefährlichen Trugschluss darstellen, denn den aktuellen Umfrageergebnissen zufolge waren immerhin 39 Prozent aller befragten Unternehmen in den vergangenen beiden Jahren von e-Crime betroffen. Zudem ist zu berücksichtigen, dass im Bereich der Computerkriminalität ein großes Dunkelfeld besteht. Die Ablehnung aufgrund vermeintlich geringer Betroffenheit verdeutlicht abermals, dass eine Verschiebung der Risikowahrnehmung weg vom eigenen Unternehmen stattfindet. Ironischerweise geben in dieser Hinsicht sogar 47 Prozent der bereits betroffenen Unternehmen an, dass sie aus diesem Grund keine Cyber-Versicherung abgeschlossen haben.

Abb. 39: Begründung für Verzicht auf Cyber-Versicherung
Angaben in Prozent



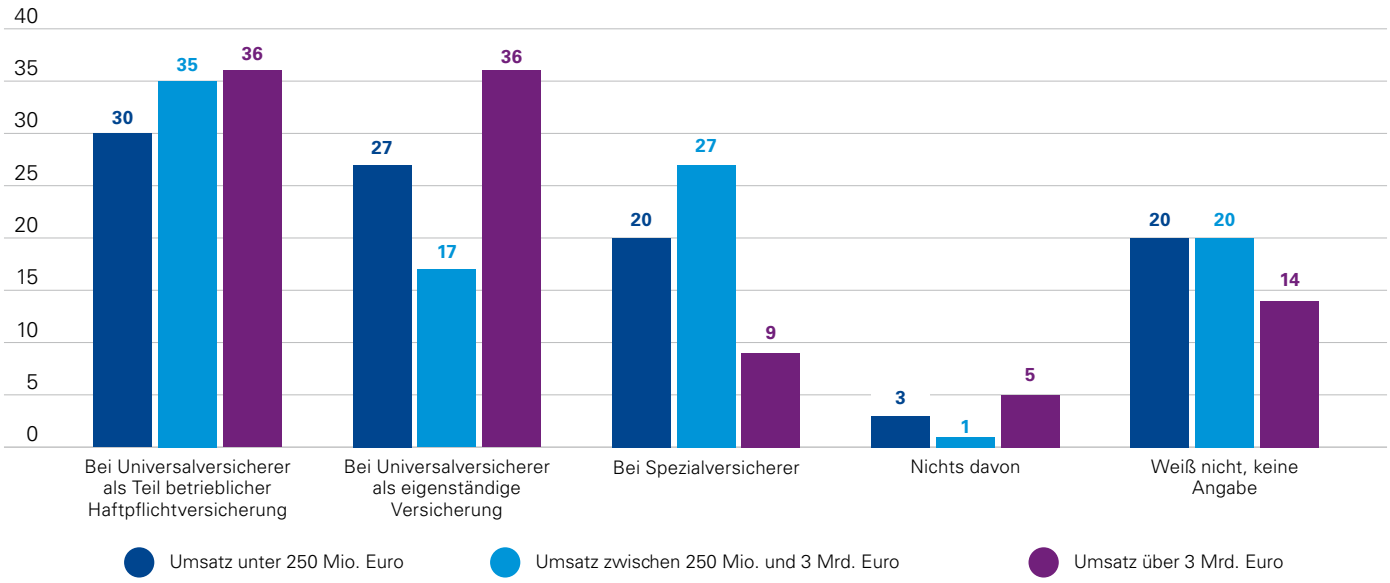
Quelle: KPMG in Deutschland, 2019

Die Hälfte der Befragten beklagt darüber hinaus ein ungünstiges Kosten-Nutzen-Verhältnis und verzichtet daher auf den Versicherungsschutz. Alle potenziell im Zusammenhang mit e-Crime anfallenden Kosten – zum Beispiel durch den Abfluss von Vermögenswerten oder entgangenen Gewinn infolge von Betriebsausfällen, aber auch für Aufklärungsmaßnahmen oder einen Rechtsbeistand – können die Kosten für die Police unter Umständen jedoch schnell übersteigen. Die Kompensation einer Versicherungspolice sollte daher nicht unterschätzt werden. Allerdings gilt es zu berücksichtigen, dass vor allem bereits betroffene Unternehmen diesen Grund für einen Verzicht angeben (57 Prozent; nicht Betroffene: 43 Prozent). Sie sind eher in der Lage, tatsächliche Kosten und den Preis einer Versicherungspolice zu vergleichen, was ihnen durchaus eine qualifizierte Aussage zum Kosten-Nutzen-Verhältnis ermöglichen dürfte.

Ein zu hoher Aufwand für die Beurteilung der eigenen Risiken sowie ein Mangel an Ressourcen werden von weniger als einem Drittel der Befragten genannt. Darüber hinaus geben 17 Prozent an, nicht über ein ausreichendes Verständnis der Versicherungsleistung zu verfügen.

Etwas mehr als jedes fünfte Unternehmen, das über eine Cyber-Versicherung verfügt, hat diese Police bei einem Spezialversicherer abgeschlossen (Abb. 40). Dies trifft insbesondere auf kleine und mittlere Unternehmen zu (20 beziehungsweise 27 Prozent). Hingegen haben 72 Prozent der „Großen“ ihren Vertrag mit einem Universalversicherer geschlossen – jeweils 36 Prozent von ihnen als Teil der betrieblichen Haftpflichtversicherung oder aber als eigenständige Police. Etwa ein Fünftel der Befragten hat diese Frage nicht beantwortet.

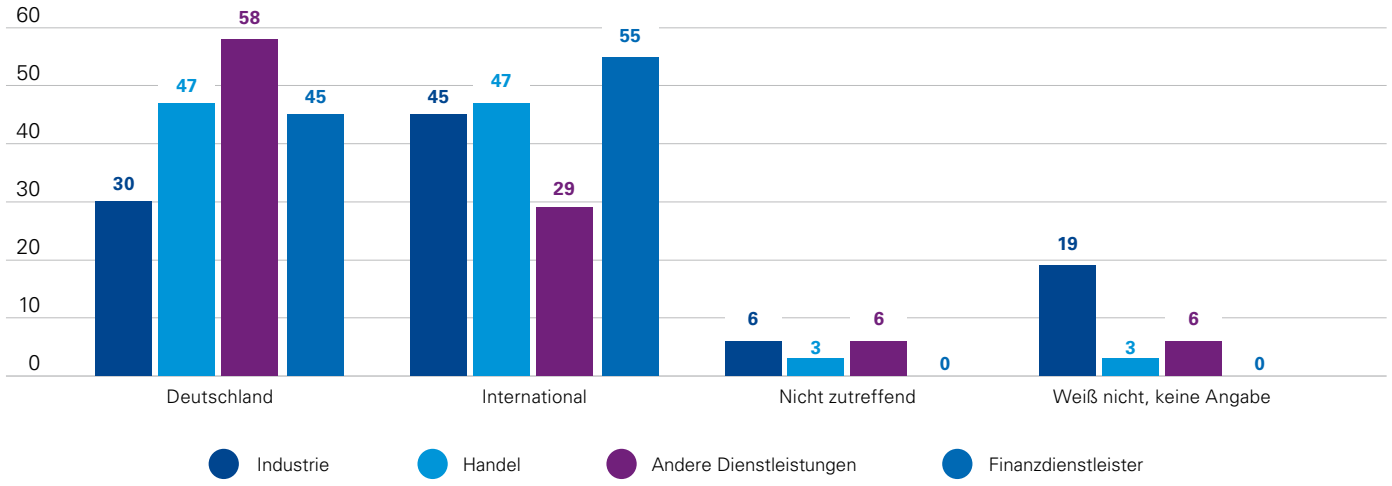
Abb. 40: Versicherungsgeber
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Hinsichtlich der Reichweite der Versicherung halten sich eine auf Deutschland beschränkte und eine internationale Abdeckung ungefähr die Waage (46 zu 41 Prozent (Abb. 41)). Es ist wenig überraschend, dass die Häufigkeit der internationalen Abdeckung mit der Unternehmensgröße zunimmt – schließlich spielen Auslandstätigkeiten bei einem Global Player eine wesentlich größere Rolle als beispielsweise bei einem kleinen Mittelständler. So verfügen knapp zwei Drittel der großen Unternehmen über eine Police mit internationaler Abdeckung, wohingegen dies nur bei 29 Prozent der kleinen der Fall ist.

Abb. 41: Nationale/internationale Abdeckung
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Bei der Frage nach der Nutzung der Versicherung zeigt sich, dass große Unternehmen diese deutlich häufiger in Anspruch genommen haben als die übrigen Befragten (18 gegenüber 3 beziehungsweise 4 Prozent). Dies deckt sich mit den Ergebnissen der vorigen Studie. Insgesamt mussten bislang nur 6 Prozent der Unternehmen auf ihre Cyber-Versicherung zurückgreifen. Zu klären wäre hier, ob Unternehmen ihrer Versicherung nur Fälle bestimmter Größe oder Art melden und kleinere Angelegenheiten eher in Eigenregie bearbeiten.

Aufgrund der geringen Fallzahlen zu gemeldeten Schäden in dieser sowie der vorigen Studie sind Aussagen zur Schadenssumme und zu den in Anspruch genommenen Versicherungsleistungen kaum möglich. Die beanspruchten Leistungen beinhalten zum Beispiel die Übernahme von Eigen- und Fremdschäden, die Kompensation von Kosten für die Benachrichtigung Betroffener oder auch für Betriebsunterbrechungen, aber unter anderem auch Aspekte der Sachverhaltsaufklärung, was nicht zuletzt Kosten für externe IT-Forensiker oder -Experten, die Erstaufklärung und die Rechtsverfolgung einschließt.

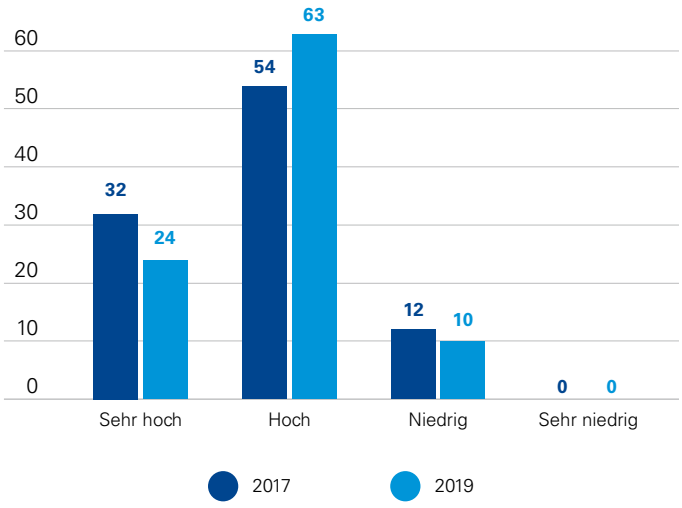
Infektion braucht Diagnose

06 Ransomware

Ein Mitarbeiter erhält eine E-Mail, klickt auf den enthaltenen Link oder Anhang – und sofort werden die Dateien auf seinem Computer durch einen Trojaner verschlüsselt.[4] Der gängige Begriff für solche Schadprogramme lautet Ransomware – oder auch Verschlüsselungs-, Erpressungs- oder Kryptotrojaner. Im Austausch dafür, dass die Dateien angeblich wieder entschlüsselt werden, wird der Mitarbeiter aufgefordert, ein Lösegeld zu zahlen, in der Regel in Form von Bitcoins oder einer anderen nicht oder kaum verfolgbaren Kryptowährung. Dabei besteht allerdings keine Gewissheit, dass der Zugriff auf die Dateien nach der Zahlung wieder gewährt wird. Prominente Beispiele für solche „digitalen Erpressungen" in großem Stil sind die Schadprogramme Locky, WannaCry und NotPetya. Die Folgen von Ransomware-Angriffen sind nicht nur der Abfluss des Lösegelds, sondern oft auch der Verlust der Daten sowie Einschränkungen der Produktivität eines Unternehmens, die bis hin zu vollständigen Betriebsausfällen führen können.

Entsprechend groß ist das Risiko, das die Befragten mit Blick auf Ransomware wahrnehmen. So schätzen 87 Prozent das Risiko, solcher Schadsoftware ausgesetzt zu sein, als hoch oder sehr hoch ein, wobei die Kategorie „sehr hoch" von immerhin 24 Prozent gewählt wird (Abb. 42). Die deutlichste Veränderung gegenüber der Befragung des Jahres 2017 liegt jedoch im Bekanntheitsgrad. Damals gab etwa die Hälfte der Befragten an, das Phänomen Ransomware – zu diesem Zeitpunkt keineswegs aus dem Nichts kommend – sei ihnen nicht geläufig. Dies gibt in diesem Jahr weniger als 1 Prozent der Befragten an, was unterstreicht, welch große Aufmerksamkeit derartige Angriffe in jüngster Zeit erlangt haben.

Abb. 42: Risikowahrnehmung Ransomware
Angaben in Prozent

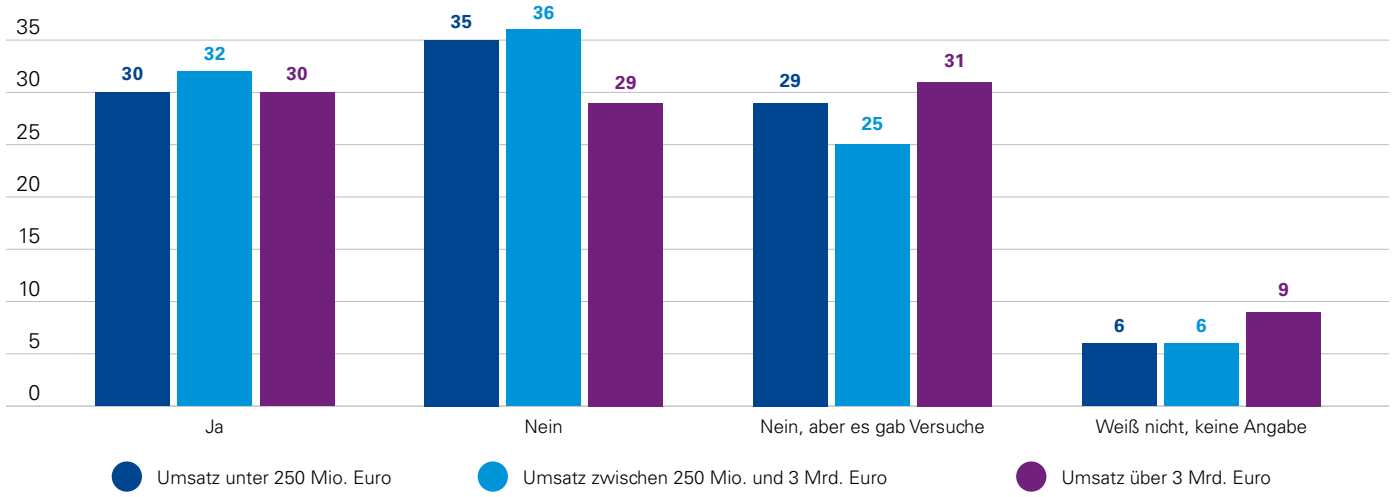


Quelle: KPMG in Deutschland, 2019

Tatsächlich war knapp ein Drittel der Befragten mit Ransomware konfrontiert. Weitere 28 Prozent konnten Angriffe abwehren, bevor diese zum Erfolg führten. Insbesondere bei großen Unternehmen zeigt sich im Vergleich zur Vorgängerstudie ein deutlicher Anstieg bei der Zahl der Attacken. So hat sich der Anteil der Betroffenen verdoppelt – der diesjährigen Befragung zufolge war dies bei etwa jedem dritten großen Unternehmen der Fall (Abb. 43) und auch jedes dritte kleine und mittlere Unternehmen war betroffen.

[4] Systeme können auch anderweitig infiziert werden, zum Beispiel mit sogenannter Huckepack-Schadsoftware.

Abb. 43: Betroffenheit durch Ransomware
Angaben in Prozent

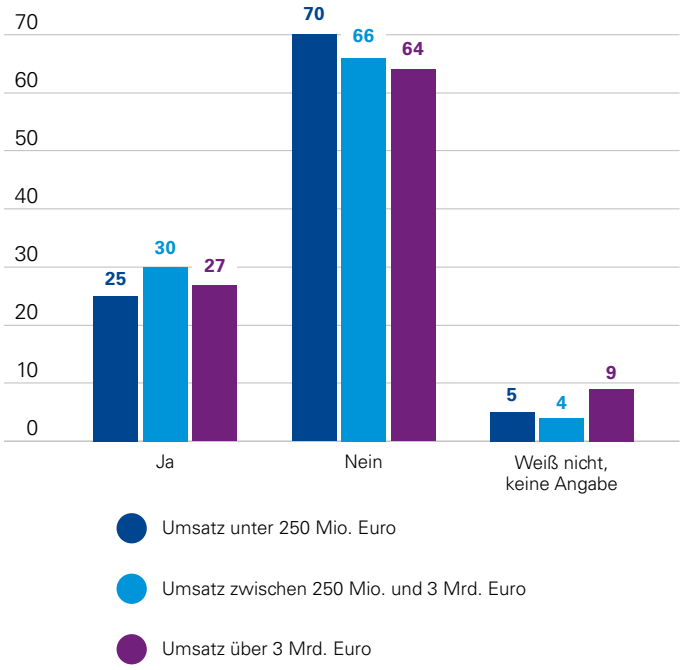


Quelle: KPMG in Deutschland, 2019

In vielen Fällen sind die von Ransomware verursachten Schäden relativ gering. So liegen rund 50 Prozent der Gesamtschäden in einem Bereich von bis zu 10.000 Euro. Dies zeigt, dass solche Angriffe nicht immer zu einer gravierenden Beeinträchtigung führen und Systeme gegebenenfalls schnell wiederhergestellt werden können sowie der Betrieb wieder aufgenommen werden kann. Allerdings nennen immerhin über 12 Prozent der Betroffenen Kosten von 50.000 Euro und 2 Prozent gar von über 500.000 Euro. In den Medien wurde zudem über Fälle berichtet, die zu einem Gesamtschaden in dreistelliger Millionenhöhe geführt haben. Ein Mangel an entsprechenden Präventionsmaßnahmen birgt daher ein hohes finanzielles Risiko, zumal die Aufarbeitung eines Vorfalls Wochen oder sogar Monate dauern kann.

Insgesamt erlitt jedes vierte Unternehmen einen Betriebsausfall durch einen Ransomware-Angriff (Abb. 44). Eine branchenspezifische Betrachtung zeigt, dass insbesondere der Handel mit 37 Prozent überdurchschnittlich von Betriebsausfällen betroffen ist. Dies könnte daran liegen, dass Unternehmen dieser Branche mit Einkauf und Vertrieb im Wesentlichen lediglich zwei starke Säulen haben, womit ein Ransomware-Angriff auf einen der beiden Bereiche gleich ein Herzstück des Unternehmens lahmlegt. Im Gegensatz dazu kam es lediglich bei 15 Prozent der Finanzdienstleister nach Ransomware-Angriffen zu einem Betriebsausfall.

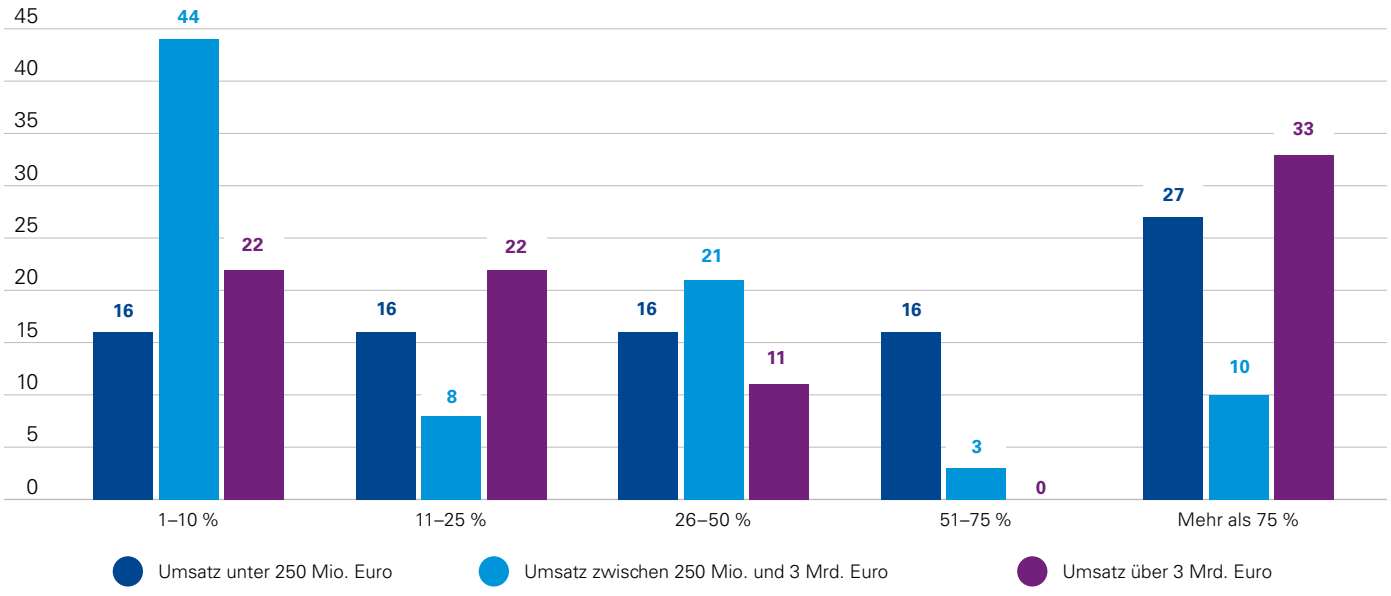
Abb. 44: Betriebsausfall infolge von Ransomware
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Bei den Unternehmen, bei denen Ransomware einen Betriebsausfall verursacht hat, waren durchschnittlich 40 Prozent der IT-Landschaft betroffen (Abb. 45). Bei jedem fünften Unternehmen betraf der Ausfall sogar mehr als 75 Prozent der gesamten IT-Landschaft. Hierin offenbart sich das enorme Gefahrenpotenzial von Ransomware. Wird ein Angriff nicht konsequent abgewehrt, kann dies erhebliche Schäden unterschiedlichster Art nach sich ziehen – Lösegeldzahlungen, Betriebsausfälle oder auch eine langwierige Aufarbeitung des Sachverhalts, um nur die gravierendsten zu nennen.

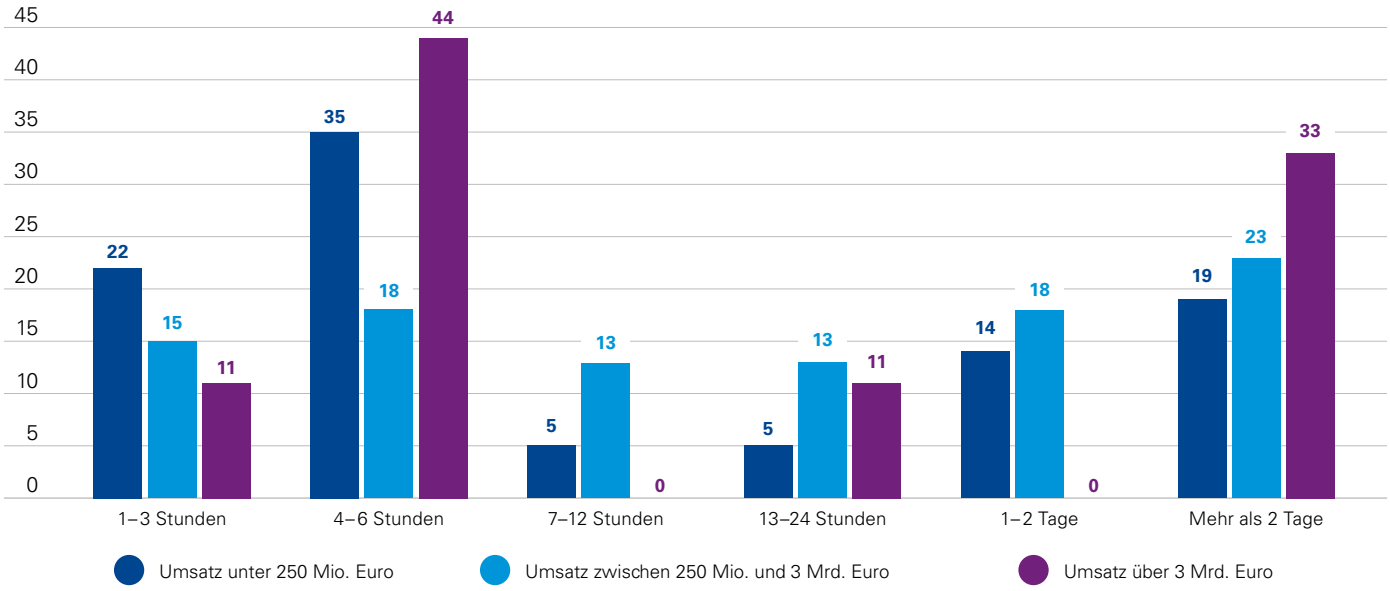
Abb. 45: Betroffene IT bei Betriebsausfall
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

Die Schäden summieren sich, je länger ein Betriebsausfall andauert und die betroffene IT nicht wieder in Betrieb genommen werden kann. Die Dauer des Ausfalls kann je nach ergriffenen Präventions-, Aufdeckungs- und Aufklärungsmaßnahmen stark variieren. So war die IT einerseits etwa bei der Hälfte der Unternehmen „nur" für vier bis sechs Stunden betroffen, andererseits dauerte der Ausfall bei jedem fünften länger als zwei Tage an (Abb. 46). Durchschnittlich hielten die gemeldeten Betriebsausfälle knapp 40 Stunden an. Zudem fällt auf, dass bei einem Drittel der großen Unternehmen die Betriebsausfälle mehr als 75 Prozent der IT-Landschaft betrafen und zudem länger als zwei Tage andauerten.

Abb. 46: Dauer der Betroffenheit
Angaben in Prozent



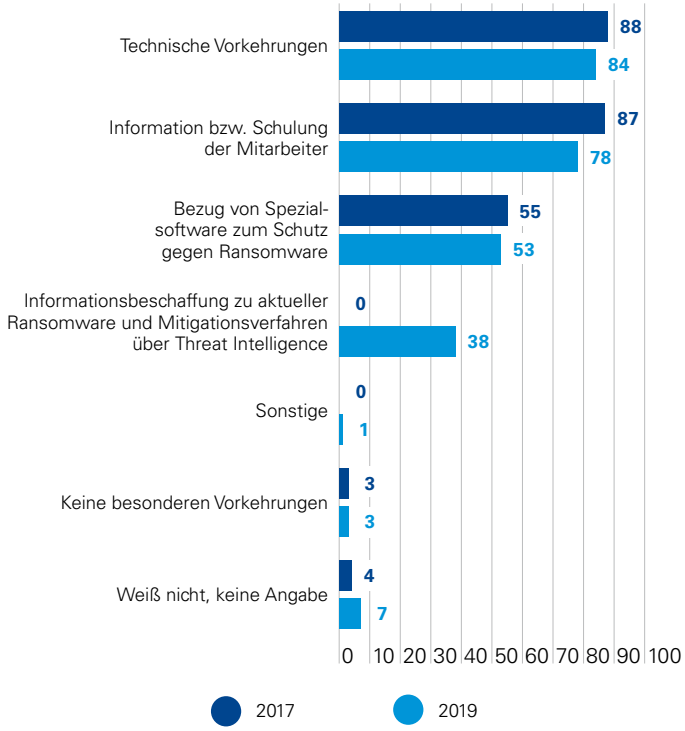
Quelle: KPMG in Deutschland, 2019

Nach wie vor sind technische Vorkehrungen wie die Anpassung der E-Mail-Filterung (84 Prozent) und die Information und Schulung der Mitarbeiter (78 Prozent) die meistgenannten Maßnahmen im Hinblick auf Ransomware (Abb. 47). Letzteres wurde in der Studie von 2017 jedoch von deutlich mehr Befragten genannt (87 Prozent). Möglicherweise ist der Rückgang mit dem generell gestiegenen Bekanntheitsgrad von Ransomware zu erklären, sodass zumindest Informationsmaßnahmen als weniger notwendig erachtet werden. Vor allem für kleine Unternehmen ist bei diesem Aspekt ein Rückgang zu verzeichnen: von 94 Prozent 2017 auf 78 Prozent bei der aktuellen Umfrage. Dabei sind entsprechende Schulungen, die Mitarbeiter für Angriffe per Phishing, Malvertising[5] oder infizierte Websites sensibilisieren, eine der wichtigsten Maßnahmen zum Schutz vor Ransomware, denn Mitarbeiter sind die Türöffner für Verschlüsselungstrojaner und somit der ausschlaggebende Faktor, ob solche Angriffe abgewehrt werden können oder nicht.

Der Trend, dass kleine Unternehmen im Vergleich zur Studie des Jahres 2017 weniger Vorkehrungen treffen, zeigt sich zum Beispiel auch bei dem Bezug von Spezialsoftware zum Schutz gegen Ransomware (Rückgang um 7 Prozentpunkte) und bei technischen Vorkehrungen wie dem Anpassen der E-Mail-Filterung (Rückgang um 8 Prozentpunkte).

[5] Als Malvertising bezeichnet man – vereinfacht gesagt – schädliche Online-Werbung, die meist dafür genutzt wird, Schadprogramme zu verbreiten.

Abb. 47: Vorkehrungen gegen Ransomware
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019

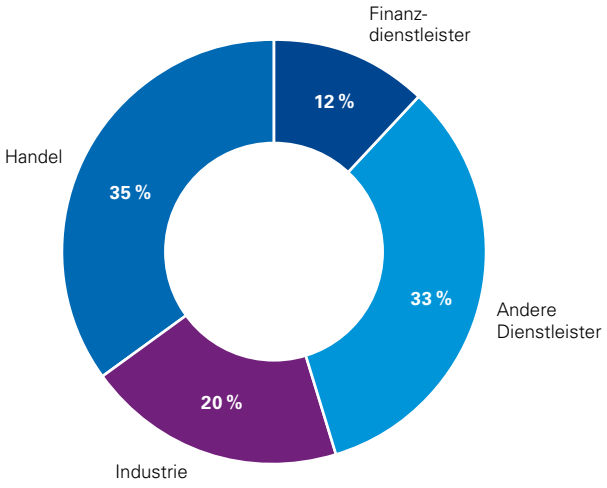
Erstaunlich ist die Vorreiterrolle, die die kleinen Unternehmen bei der Informationsbeschaffung zu Ransomware und Mitigationsverfahren über sogenannte Threat Intelligence oder beim Bezug von Spezialsoftware einnehmen. Sie nutzen derartige Optionen prozentual häufiger als Unternehmen der anderen Größenordnungen.

Reihenweise Fakten

Über diese Studie

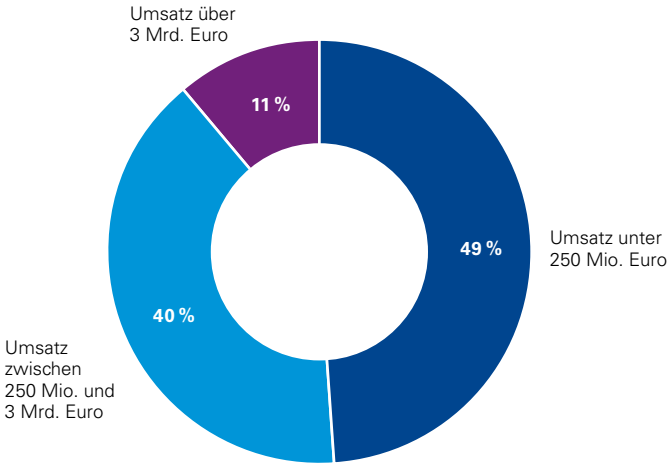
In der diesjährigen Studie wurden Vertreter von 1.001 repräsentativ nach Branche und Umsatz ausgewählten Unternehmen zu ihren Erfahrungen im Feld der Computerkriminalität befragt (Abb. 48 und Abb. 49).

Abb. 48: Befragte nach Branche



Quelle: KPMG in Deutschland, 2019

Abb. 49: Befragte nach Umsatz



Quelle: KPMG in Deutschland, 2019

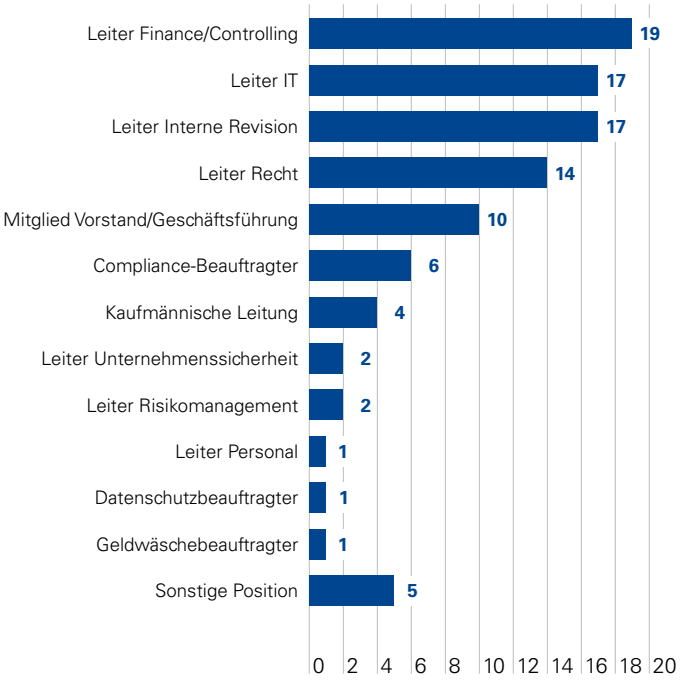
Wie bei den vorigen Ausgaben dieser Studie war das Sozialforschungsinstitut Kantar Emnid in Bielefeld mit der Durchführung der Interviews beauftragt. Die Interviews wurden telefonisch von Kantar Emnid-Mitarbeitern geführt, die im Vorfeld gezielt geschult worden waren. Die Antworten im Einzelnen wie auch die konkreten Gesprächspartner sind anonym.

Wir haben in der aktuellen Umfrage bewusst darauf verzichtet, ausschließlich IT-Abteilungen anzusprechen, denn es ging uns verstärkt darum, strategische und betriebswirtschaftliche Perspektiven auf e-Crime zu analysieren. Befragt wurden neben IT-Vertretern deshalb in erster Linie Leiter der Abteilungen Interne Revision, Rechnungswesen und Recht sowie Geschäftsführer und Vorstände (Abb. 50).

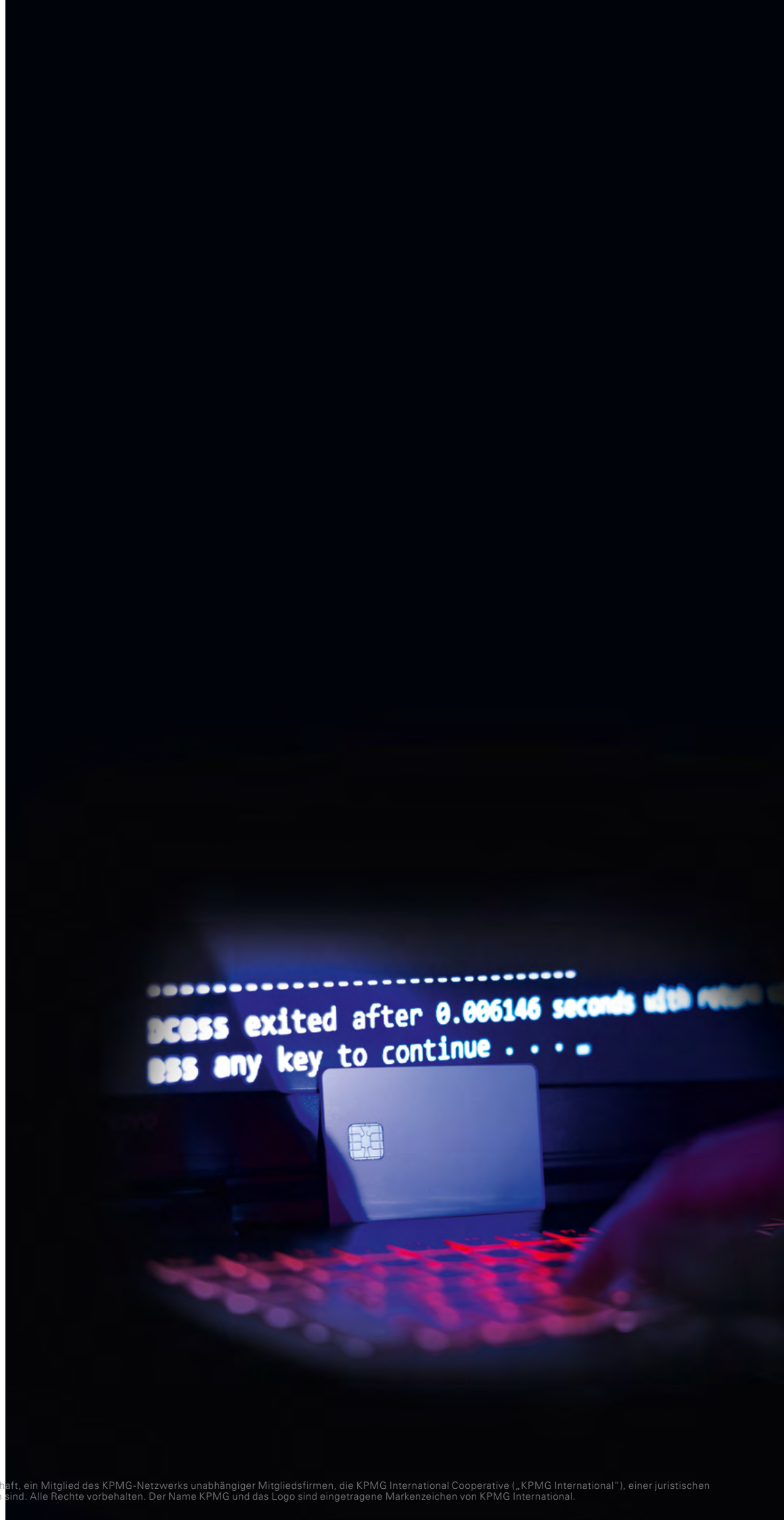
Die Erfahrung hat gezeigt, dass die Studienteilnehmer aufgrund der Komplexität des Themas eine persönliche Befragung bevorzugen. Die Interviews wurden im Zeitraum von September 2018 bis Januar 2019 geführt.

Der standardisierte Fragebogen orientiert sich an der Struktur der Vorgängerstudie, wurde jedoch hinsichtlich der diesjährigen Schwerpunktsetzung angepasst. Konzipiert wurde er vom Bereich Compliance & Forensic der KPMG AG Wirtschaftsprüfungsgesellschaft.

Abb. 50: Interviewpartner
Angaben in Prozent



Quelle: KPMG in Deutschland, 2019



Bestens für Sie aufgestellt

Über Compliance & Forensic

Der Bereich Compliance & Forensic von KPMG erbringt Leistungen rund um die Prävention, Aufdeckung und Aufklärung von Wirtschaftskriminalität und anderen Bedrohungslagen. Das Leistungsspektrum umfasst die folgenden Solutions:

Forensic Investigations
Unabhängige unternehmensinterne Ermittlungen bei Verdacht auf wirtschaftskriminelle Handlungen auf Basis erprobter Methoden.

Forensic Technology
Sofortunterstützung bei IT-Sicherheitsvorfällen sowie Krisenmanagement, Sicherung und Wiederherstellung digitaler Beweismittel sowie systematische Analyse und Auswertung von strukturierten und unstrukturierten Daten (eDiscovery).

Corporate Intelligence
Durchführung von Integrity Due Diligences zur frühzeitigen Identifikation von Integritätsrisiken bei Kunden, Subunternehmern und Geschäftspartnern.

Datenschutz
Beratung bei der Einrichtung von Datenschutz-Managementsystemen und Unterstützung bei der Reaktion auf Datenschutzvorfälle.

Geldwäscheprävention
Unterstützung bei Prävention, Aufdeckung und Aufklärung von Geldwäschevorfällen inklusive der Einrichtung von Geldwäsche-Managementsystemen.

Anti Financial Crime
Unterstützung bei der Etablierung eines Anti Financial Crime-Regimes und bei der Beseitigung kurzfristiger Problemstellungen dieser Art.

Corporate Security
Unterstützung von Mandanten im Umgang mit physischen Sicherheitsrisiken infolge von Terrorismus, organisierter und Gewaltkriminalität und politischer Unsicherheit.

Infrastructure Risk & Compliance
Unterstützung von Mandanten bei der Planung und Durchführung von Großprojekten.

Compliance Assurance
Unterstützung bei der Einrichtung und Überprüfung von Compliance Managementsystemen nach anerkannten Standards.

Compliance & Integrity Advisory
Beurteilung der Compliance-Kultur und Festlegung wesentlicher Compliance-Ziele sowie Identifikation wesentlicher Risiken und Unterstützung bei der Implementierung von Gegenmaßnahmen für den Krisenfall.

Tax Compliance
Unterstützung bei der Implementierung von Tax Compliance Managementsystemen zur Sicherstellung der Nachweisfähigkeit gegenüber den Behörden.

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

Michael Sauermann
Partner, Leiter Forensic Technology
T +49 30 2068-4624
msauermann@kpmg.com

Alexander Geschonneck
Partner, Leiter Compliance & Forensic
T +49 30 2068-1520
ageschonneck@kpmg.com

An dieser Studie haben mitgewirkt:
Jacqueline Becker und Marc Oliver Scheben

24/7-Hotline:
T 0800 SOS KPMG
T 0800 7675764

Call our hotline
T +49 202 25155 7146 (from outside Germany)

sos@kpmg.de

www.kpmg.de

www.kpmg.de/socialmedia