HISCOX

Hiscox Cyber Readiness Report 2020

Die vierte Ausgabe des internationalen Hiscox Cyber Readiness Reports wurde in Zusammenarbeit mit dem Marktforschungsunternehmen Forrester Consulting erstellt. Die Ergebnisse zeigen, wie es aktuell um das Bewusstsein von Unternehmen bezüglich Cyber-Risiken bestellt ist und wie Firmen gegen sich stetig wandelnde Cyber-Bedrohungen vorgehen wollen. Der Hiscox Cyber Readiness Report 2020 basiert auf einer repräsentativen Umfrage unter Führungskräften, Abteilungsleitern, IT-Managern und Fachexperten unterschiedlicher Branchen aus acht verschiedenen Ländern.

Cyber-Herausforderungen offensiv entgegentreten

Es gibt klare Anzeichen für einen Wandel in puncto Cyber-Readiness.

Gareth Wharton
Cyber CEO, Hiscox

Der diesjährige Hiscox Cyber Readiness Report zeigt positive Tendenzen: Nach zwei Jahren mit nur geringen Fortschritten sind Unternehmen in Sachen Cyber-Sicherheit nun besser vorbereitet. Dass sich Unternehmen verstärkt der Herausforderung stellen, zeigt sich nicht nur im Cyber-Readiness-Modell, sondern auch in Form von zunehmenden Anstrengungen und gestiegenen Ausgaben.

Dieser Fortschritt kommt keinen Augenblick zu früh. Während die Zahl der Firmen, die einen Cyber-Schadenfall melden, rückläufig ist, scheinen die Kosten und die Intensität der Cyber-Angriffe deutlich anzusteigen. Die Zahl derer, die nach einer Ransomware-Infektion ein Lösegeld bezahlt haben, ist erschreckend hoch und zeigt, dass das Problem nicht zu unterschätzen ist.

Die teilnehmenden Unternehmen wurden vor der Coronavirus-Pandemie befragt, so dass die Ergebnisse im Kontext ihrer Entstehung zu betrachten sind. Die gestiegene Anzahl gut vorbereiteter „Cyber-Experten“ zeigt, dass viele Unternehmen aktiv daran arbeiten, sich vor den stetig wandelnden Cyber-Bedrohungen zu schützen.

Das gestiegene Bewusstsein für Cyber-Gefahren allein ist keine Sicherheitsgarantie. Aber viele der unternommenen Maßnahmen, die in diesem Report ausführlich beschrieben werden, helfen Unternehmen, ihre Angriffsfläche zu reduzieren, wirksam auf Attacken zu reagieren und schnell wieder handlungsfähig zu sein. Eine gute Strategie zur Abwehr von Angriffen sowie der Aufbau einer Cyber-Resilienz – also einer Widerstandsfähigkeit gegen Cyber-Attacken – sind der Schlüssel dafür.

Als Cyber-Versicherer wissen wir, dass die Unterstützung nicht mit der Deckung eines Schadenfalls enden sollte. Umso mehr freut es uns, dass viele der „Cyber-Experten“ eine Cyber-Versicherung nicht rein zur finanziellen Absicherung nutzen. Viele haben mittlerweile erkannt, wie wichtig Assistance-Leistungen im Schadenfall sind. Mindestens genauso wichtig ist es, aus vergangenen Vorfällen zu lernen und durch Präventionsmaßnahmen die eigene Resilienz zu stärken. Der Hiscox Cyber Readiness Report zeigt, dass das ein Großteil der Experten das bereits im Alltagsgeschäft umsetzt.

Die Absicherung durch eigenständige Cyber-Versicherungen ist jedoch weiterhin lückenhaft. Mehr als die Hälfte der befragten Firmen setzt auf eine allgemeinere Abdeckung. Das wirft Fragen auf: Mit hoher Wahrscheinlichkeit sind alle befragten Unternehmen gegen Feuerschäden und Diebstahl versichert sind. Die Wahrscheinlichkeit von Cyber-Kriminellen attackiert zu werden ist laut des Report jedoch fast 20-mal höher: In Großbritannien etwa liegt diese bei 30%, im Vergleich zu 2% bei Feuer und Diebstahl.

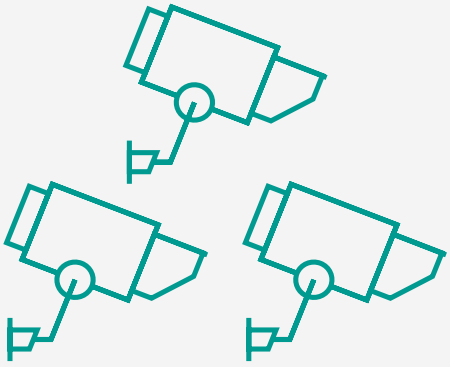
Die Ergebnisse des diesjährigen Hiscox Cyber Readiness Reports zeigen, wie wichtig es ist, dass die eigenen Mitarbeiter ihr Verhalten im Umgang mit Cyber-Risiken ändern. Zur Sensibilisierung vor Cyber-Gefahren werden mittlerweile oft unternehmensweit Schulungen abgehalten. Diese sollten Versicherer aktiv mitgestalten. Unsere Online-Schulungsplattform bietet Cyber- Schulungen für die Mitarbeiter unserer Kunden an. Mehr als 12.000 Personen haben dort inzwischen Kurse abgeschlossen. Wir stellen fest, dass Teilnehmer dann Verstöße oft schneller erkennen und uns benachrichtigen. So können wir dabei helfen, dass sie ihre Arbeit schneller und effektiver wieder aufnehmen können.

Cyber Readiness hat viele Facetten. Wir hoffen, dass der diesjährige Report mit zahlreichen Best-Practice-Beispielen Unternehmen helfen wird, diese Herausforderung besser zu verstehen und angemessen darauf zu reagieren.

Zusammenfassung
Es gibt ein neues Bewusstsein für die Cyber-Herausforderung.

Ein neues Gefahrenbewusstsein
Unternehmen sind sich der Herausforderung durch Cyber-Gefahren zunehmend bewusst.

Sprunghafter Anstieg der Ausgaben
Insgesamt erhöhten die Firmen ihre Ausgaben für Cyber-Sicherheit um 39%. Die sogenannten „Cyber-Experten“ gaben noch mehr aus und planen, dies auch in Zukunft zu tun.



Unternehmen haben höhere Schäden
Die gesamten Cyber-Verluste der betroffenen Unternehmen beliefen sich auf 1,6 Milliarden € im Vorjahr.

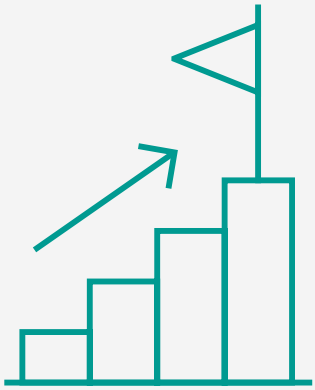
Cyber-Verluste schießen in die Höhe
Die Kosten nach einem Angriff stiegen fast um das Sechsfache auf einen Medianwert von 50.000 € an.

Zahl der Cyber-Attacken nimmt ab

Die Zahl der von einem Cyber-Vorfall betroffenen Firmen fiel von 61% auf 39%.

Höchster verzeichneter Verlust

Die höchsten Cyber-Verluste wurden von einem britischen Finanzdienstleistungsunternehmen gemeldet: 79.9 Millionen €.



Lösegeld-Erpressungen

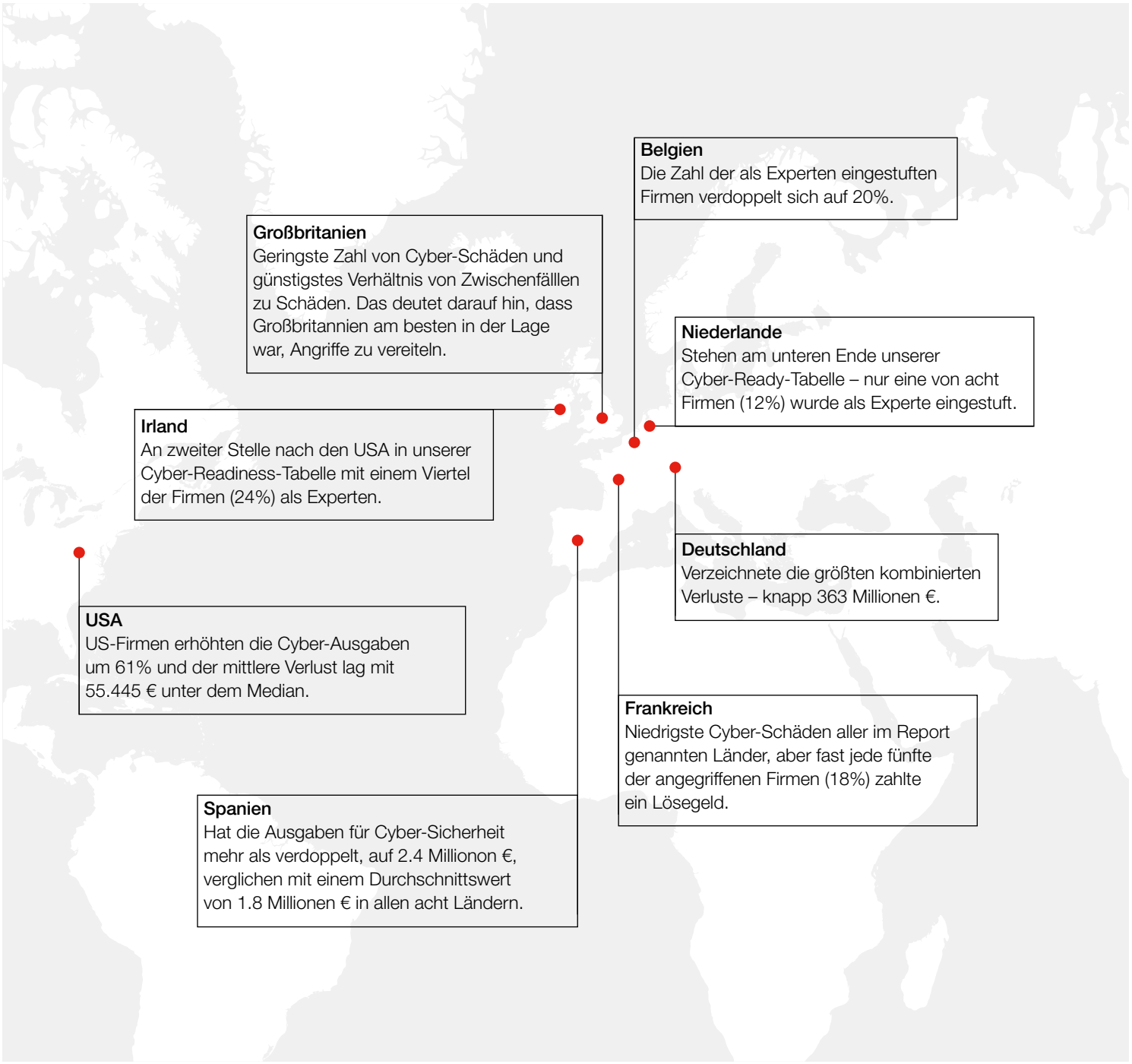
Mehr als 6% der Unternehmen zahlten ein Lösegeld: Die Lösegeldsumme belief sich bei den 350 Firmen zusammen auf 335 Millionen €.

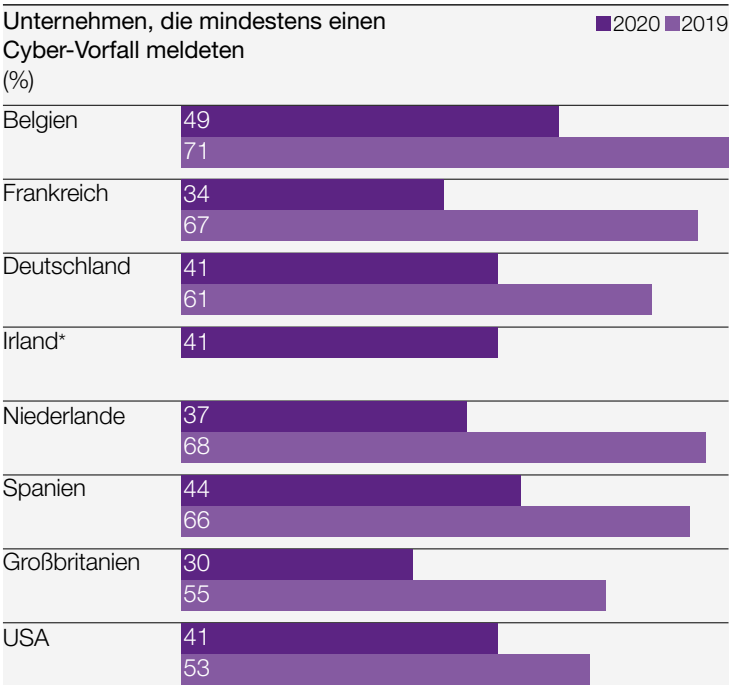
Positive Signale

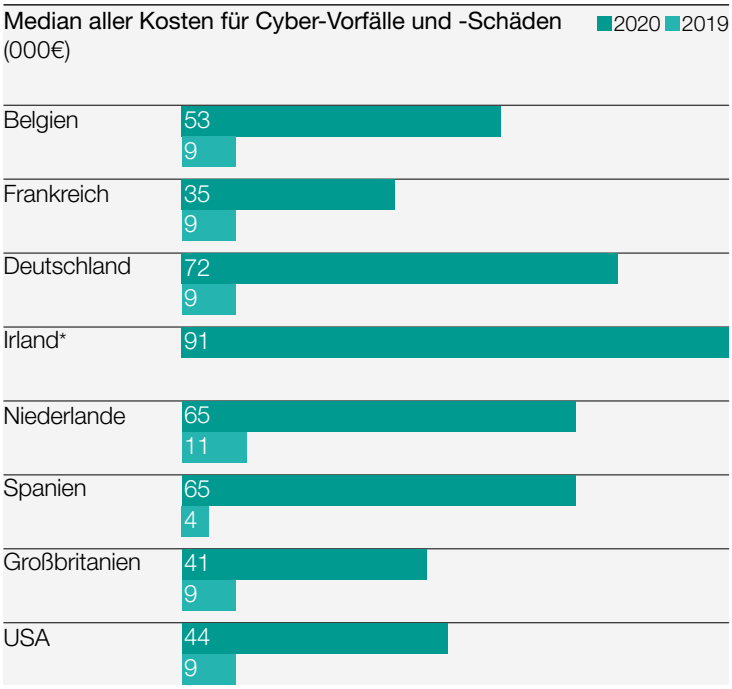
Doppelt so viele Unternehmen reagierten auf einen Cyber-Schaden, indem sie neue Sicherheitsmaßnahmen etablierten und mehr für die Schulung der Mitarbeiter ausgaben.

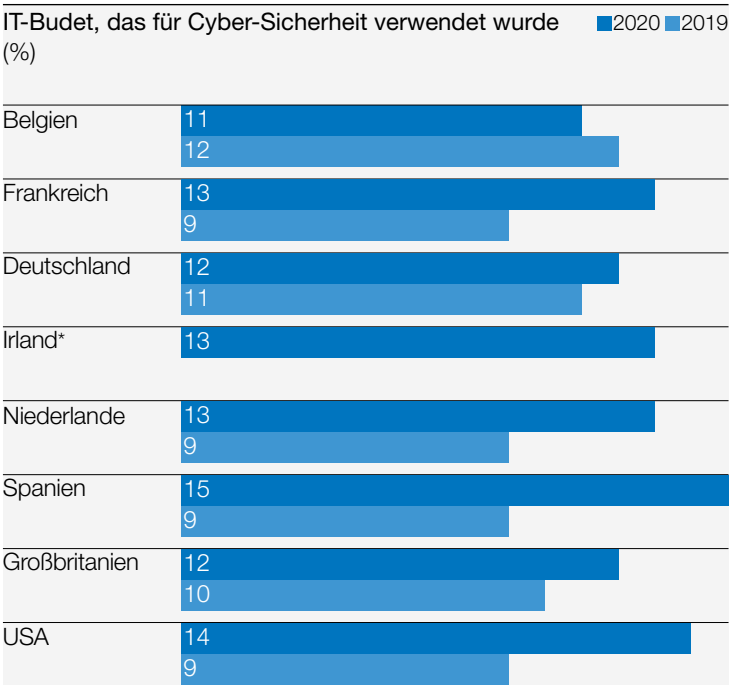
Länderübersicht

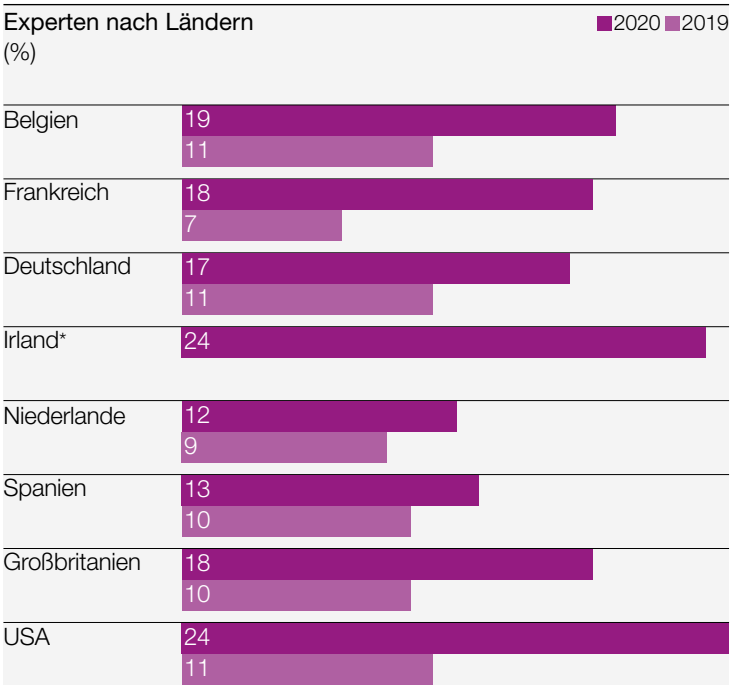
Die Kosten für Cyber-Vorfälle und Investitionen in die Sicherheit steigen weltweit.











*Daten nur für 2020 verfügbar.

Die Größenordnung des Problems

Während eine kleinere Anzahl von Unternehmen Cyber-Angriffe verzeichnete, stiegen die Kosten in die Höhe.

Weniger Zwischenfälle, größere Schäden
Der Anteil der Firmen, die in den vergangenen 12 Monaten über einen Cyber-Angriff berichteten, ist in diesem Jahr von 61% auf 39% gesunken. Das ist die gute Nachricht. Die schlechte Nachricht ist, dass die finanziellen Auswirkungen um ein Vielfaches größer sind als zuvor.

Ein oder mehrere Cyber-Ereignisse wurden gemeldet

Erstmals baten wir die Unternehmen, die Anzahl Ihrer der Cyber-Angriffe und -Schäden (siehe Definitionen auf S. 9) getrennt zu quantifizieren, was eine detailliertere Analyse der Cyber-Resilienz der Unternehmen ermöglichte.

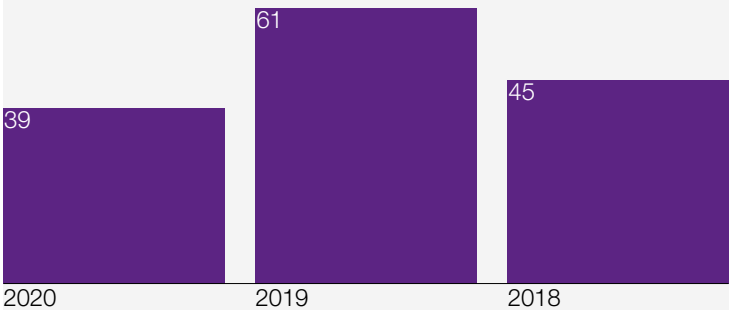
Unter denjenigen, die über einen Cyber-Zwischenfall der einen oder anderen Art berichteten, lag die mittlere Anzahl bei 50. Der Median lag bei 15 Schäden. Belgische und deutsche Firmen waren die Hauptziele, mit Medianwerten von 100 bzw. 80 Angriffen. Bei den Schäden war es andersherum, was darauf hindeutet, dass deutsche Firmen weitaus weniger erfolgreich bei der Abwehr der Hacker waren. Betrachtet man das gesamte Spektrum der Befragten (einschließlich derjenigen, die kein Cyber-Zwischenfall meldeten oder "weiß nicht" angaben), so verzeichnete das durchschnittliche Unternehmen 20 Attacken und sechs Schäden.

Entstehung von "Superzielen"
Die Zahlen wurden stark durch eine relativ kleine Zahl von Firmen in jedem der acht Länder beeinflusst, die 500 oder mehr Cyber-Zwischenfälle in jeder Kategorie meldeten. Sie entstanden aufgrund einer Änderung unseres Fragebogens in diesem Jahr, die es den Befragten ermöglichte, eine offene Antwort auf die Anzahl der Cyber-Vorfälle zu geben, die sie erlitten hatten.

Es wäre plausibel, anzunehmen, dass es sich bei allen um Großunternehmen handelt. Doch ist das nicht der Fall (siehe Grafik). Es gibt Superziele in jeder unserer fünf Größenklassen. Eine überraschende Zahl von ihnen gehört zu den kleinsten Unternehmen.

Es gibt viele mögliche Gründe für diese Zahlen. In vielen Branchen hat die Mehrheit der Kleinstunternehmen niemanden, der sich dezidiert um die Cybersicherheit kümmert. Die kleinen Transport- und Vertriebsfirmen scheinen besonders anfällig: 59% sagen, dass sie weder intern noch extern jemanden in eine solchen Position hätten. Ebenso kann die Abhängigkeit von einem externen Dienstleister nach hinten losgehen, wenn dieser selbst angegriffen wird. Einige Firmen haben womöglich zu hohe Zahlen angegeben, indem sie Spam-E-Mails einbezogen.

Ein oder mehrere Cyber-Angriffe wurden gemeldet von
(%)



Das Fehlen wirksamer Gegenmaßnahmen bei einigen kleineren Unternehmen ist eine weitere Erklärung dafür. Die Analyse der Daten deutet darauf hin, dass Firmen mit weniger als 12 Computern, bei denen keine einheitliche Antiviren-/Anti-Spyware-Software im gesamten Unternehmen eingesetzt wurde, besonders häufig zu den Superzielen gehörten.

Dennoch waren die Großunternehmen häufiger ein Ziel als kleinere Unternehmen. Mehr als die Hälfte aller großen Unternehmen (51%) – also jene mit mehr als 1000 Mitarbeitern - gaben an, mindestenseinen Cyber-Zwischenfall verzeichnet zu haben. Sie vermeldetenauch bei weitem die meisten Cyber-Attacken (mit einem Medianwertvon 100) und -Schäden (80). Sie wurden mit ziemlicherWahrscheinlichkeit stärker ins Visier genommen, aber wahrscheinlichwaren sie auch besser in der Lage, Angriffe zu erkennen.

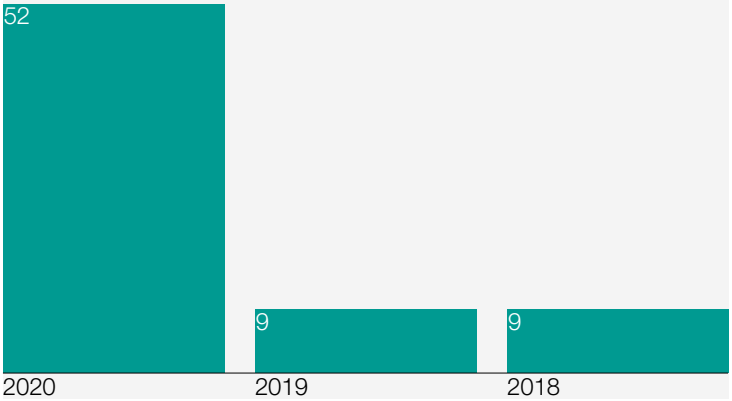
Das Versäumnis, ausreichend in Cybersicherheit zu investieren, scheint allen Superzielen gemein zu sein. In den meisten Branchen waren es jene großen Firmen mit mehr als 700 Computern, die weniger als 8% ihres IT-Budgets für die Cybersicherheit ausgaben, die zu Superzielen wurden.

Die am stärksten angegriffenen Branchen waren Finanzdienstleistungen, Fertigung und TMT – 44% der Firmen in jedem Sektor berichteten über mindestens eine Attacke oder einen Schaden. Ironischerweise waren dies gleichsam die drei Branchen, die in unserem Cyber-Readiness-Report am besten abschnitten, aber Unternehmen sind oft gezwungen, Cyber-Experten zu werden, wenn es sich um stark attackierte Branchen handelt.

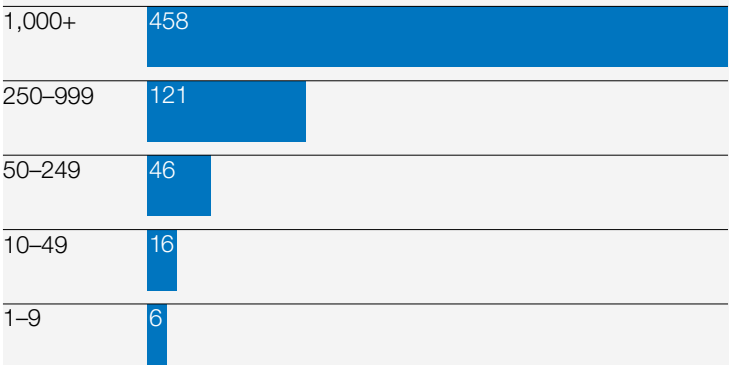
1,6 Milliarden €

Gesamtkosten entstanden den befragten Unternehmen aufgrund von Cyber-Vorfällen in den letzten 12 Monaten Monaten.

Mediane Kosten aller Cyber-Vorfälle
(000€)



Gesamtkosten aller Cyber-Vorfälle nach Unternehmensgröße
Mitarbeiter (000€)



Viele antworteten: "Weiß nicht"
Beunruhigend ist, dass 11% der Befragten insgesamt angaben, sie wüssten nicht, wie oft sie attackiert wurden. Das waren mehr als 4% im Vorjahr. Überraschenderweise wurde "weiß nicht" am häufigsten von Unternehmen mit 1000+ Angestellten (15%) geantwortet.

Es ist erwähnenswert, dass der Rückgang des Gesamtprozentsatzes der Firmen, die einen Cyber-Zwischenfall melden, möglicherweise auf die stärkere Gewichtung von Kleinstunternehmen in der diesjährigen Studiengruppe zurückzuführen ist. Etwa 63% der Unternehmen mit weniger als zehn Mitarbeitern gaben an, dass sie überhaupt keine Cyber-Vorfälle oder -Verletzungen zu verzeichnen haben. Aber fast die Hälfte (49%) hatte keine definierte Rolle für die Cybersicherheit – was darauf hindeutet, dass sie “tote Winkel” haben könnten.

Die Kosten stiegen rasant – auf fast 1,6 Millarden €
Die diesjährigen Zahlen veranschaulichen den Preis, der heute für eine Online-Präsenz zu zahlen ist. Der Median der Kosten für die 1.971 Unternehmen, die von Cyber-Attacken und -Schäden betroffen waren und die die Aufwendungen in den letzten 12 Monaten nachhielten, lag bei 51.200 €. Das ist fast eine Versechsfachung gegenüber den 9.000 € des Vorjahres.

Mediane Kosten aller Cyber-Vorfälle

Rechnet man die Kosten aller von unserer Studiengruppe gemeldeten Cyber-Vorfälle zusammen, so belaufen sich die Gesamtkosten auf 1,6 Milliarden €. Dies steht im Vergleich zu 1,1 Milliarden € im Vorjahr, als die Zahl der angegriffenen Unternehmen fast 33% höher war.

Wer war am stärksten gefährdet?
Kurz gesagt, es waren die größeren Unternehmen, die den höchsten Preis zahlten. Dies sollte nicht überraschen, da sie auch am stärksten ins Visier genommen wurden.

Gesamtkosten aller Cyber-Vorfälle nach Unternehmensgröße

Hinter den Medianwerten sind die finanziellen Auswirkungen je nach Land, Sektor und Unternehmen sehr unterschiedlich. Der höchste verzeichnete Gesamtverlust für ein einzelnes Unternehmen belief sich auf 79,9 Milliarden € (ein britisches Finanzdienstleistungsunternehmen), während der höchste Verlust durch einen einzelnen Cyber-Angriff 14,4 Milliarden € (ein britisches Berufsdienstleistungsunternehmen) betrug. Dem steht ein Median der Kosten für den größten Einzelvorfall steht ein Median von nur 3.700 € gegenüber.

Größter Schaden

Irische und deutsche Firmen erlitten die größten Verluste im Median, aber Schäden waren weit verbreitet. Unter den attackierten Firmen stiegen die durchschnittlichen Kosten für Energieunternehmen um mehr als das Dreißigfache, während mehrere andere Sektoren mit Verlusten zu kämpfen hatten, die um ein Vielfaches höher lagen als im Vorjahr (siehe Tabelle). Die Zahlen deuten darauf hin, dass Cyberkriminelle Energie- und Fertigungsfirmen zunehmend als lukrative Ziele betrachten.

Branchen mit den höchsten Schäden

Die Hiscox Sicht

Wir haben in den letzten sechs bis zwölf Monaten eine Veränderung im Verhalten der Hacker registriert, da sie sich mehr auf Branchen wie Energie und Fertigung konzentrieren. Wir glauben, dass es dafür drei Gründe gibt: 1. Hohe Abhängigkeit von der Automatisierung (von Computern gesteuert); 2. Niedriger Grad der Cyber-Resilienz (unzureichende Backups, eingeschränkte Notfallwiederherstellungsplanung/-tests); 3. Angesichts dessen eine geringe Widerstandfähigkeit gegenüber oft großflächigen Ausfällen, weswegen diese Branchen eine reiche Beute für Lösegeld-Erpresser.

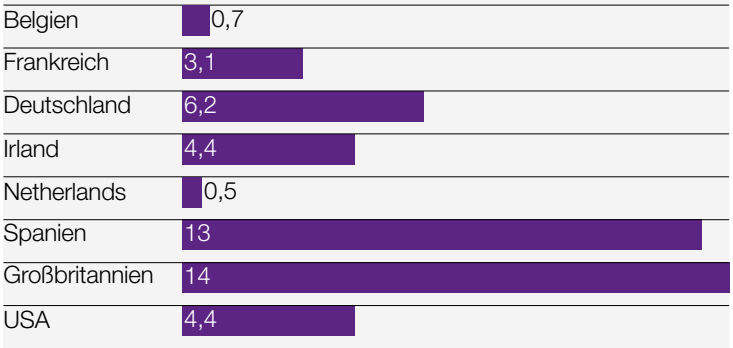
Ransomware: Ein lukratives Geschäft

Die diesjährigen Daten geben einen erschreckenden Einblick in die Kosten und die Häufigkeit von Malware- und Lösegeldangriffen. Wir baten die Befragten, die Art der Attacken und Schäden, die sie erlitten haben, genauer zu beschreiben.

Häufigste Arten von Cyber-Angriffen

In den meisten Kategorien verzeichneten große Unternehmen mit größerer Wahrscheinlichkeit Cyber-Vorfälle als kleinere Firmen. Das kann daran liegen, dass sie lukrativere Ziele waren oder auch einfach besser in der Lage waren, Angriffe zu identifizieren.

Größter Schaden
(m€)



Branchen mit den höchsten Schäden
Mediane Verluste (€)

	2020	2019
Energie	306,000	9,000
Produzierendes Gewerbe	91,000	11,000
Finanzdienstleistungen	151,000	27,000
TMT	69,000	9,000
Pharma	55,000	9,000

Häufigste Arten von Cyber-Angriffen
(%)

350

der befragten Firmen gaben an, nach einem Ransonware- oder Malware-Angriff Lösegeld gezahlt zu haben.

Malware- und Ransomware-Angriffe
Angriffe und Schadenfälle

	Malware ohne Ransomware	Malware mit Ransomware
Zahl der Angriffe	173	411
Mittlere Kosten	447,000€	843,000€
Maximale Verluste für einzelnes Unternehmen	9,2m€	46m€
Größter Einzelverlust	1,4m€	6,4m€
Verluste insgesamt	77m€	346m€

Die dramatischsten Zahlen betreffen Malware- und Lösegeld-Angriffe. Insgesamt zahlten 350 Firmen (d.h. etwa jede sechste Firma, die von einem Cyber-Zwischenfall berichtete - 16%) nach einem Ransomware-Angriff ein Lösegeld.

Ob ein Lösegeld gezahlt wurde oder nicht - die mittleren Kosten für alle Firmen, die einem Ransomware-Angriff ausgesetzt waren, waren fast doppelt so hoch wie für diejenigen, die sich nur mit einer Malware allein auseinandersetzen mussten - 821.000 € im Vergleich zu 436.000 €. Die höchsten Gesamtkosten für ein einzelnes Unternehmen, Lösegeld und andere Kosten zusammengerechnet, lagen bei 44,8 Millionen €.

Malware- und Ransomware-Angriffe

Diese Zahlen verdeutlichen, wie wichtig eine gute Erkennung von Cyber-Gefahren ist, bevor aus Malware Lösegeldforderungen werden. Unter den Firmen, die über jegliche Form von Cyber-Ereignissen berichteten, hatten die USA und Frankreich den höchsten Prozentsatz an Lösegeldzahlungen zu verzeichnen (18% gegenüber einem Durchschnitt von 16%). Die gute Nachricht ist, dass eine große Anzahl von Firmen angab, ihre Daten entweder von einem Backup wiederherzustellen oder sie ohne Lösegeldzahlung wieder aufzubauen (19% bzw. 17%).

Die Hiscox Sicht

Wir sehen, wie sich die Ransomware-Techniken der Hacker weiterentwickeln. Typischerweise gibt es bei größeren Angriffen zwei unterschiedliche Phasen nach der Erstinfektion: Seitliche Bewegung - die Angreifer suchen nach wertvollen Vermögenswerten (HR, Finanzdaten) und schätzen die Anzahl der Ziele ein, um die Höhe des Lösegeldes festzulegen; Ransomware-Angriff - dies geschieht oft am Wochenende, wenn die Reaktionsmöglichkeiten geringer sind und die Hacker daher den größten Schaden anrichten können. Zwischen diesen beiden Phasen kann in der Regel ein Zeitraum von ein bis drei Wochen liegen. Unternehmen mit guten Detektionsfähigkeiten können den Angriff innerhalb dieser Zeit stoppen und erleiden daher kürzere Ausfälle, geringere Gesamtkosten und geringere Auswirkungen auf das Geschäft.

Längerfristige Auswirkungen

Die weicheren Auswirkungen eines Cyberschadens werden oft nicht erwähnt oder sind einfach zu schwer zu quantifizieren. Ihre Tragweite sollte aber nicht unterschätzt werden. Deutlich mehr Befragte nannten in diesem Jahr entweder erhöhte Schwierigkeiten bei der Gewinnung neuer Kunden (15 % der Unternehmen, die ins Visier genommen wurden, im Vergleich zu zuvor 5 %), den tatsächlichen Verlust von Kunden (11 % im Vergleich zu zuvor 5 %) oder den Verlust von Geschäftspartnern (12 % im Vergleich zu 4 %).

Nahezu jedes fünfte französische Unternehmen (19%) berichtete von größeren Schwierigkeiten, nach einem Zwischenfall oder einem Verstoß Kunden zu gewinnen. Etwa 16% der belgischen Unternehmen haben Geschäftspartner verloren (im Vergleich zu einem Mittelwert von 12%).

Insgesamt gaben 15 % der betroffenen Unternehmen an, die Cybersicherheit ihrer Lieferkette neu bewertet zu haben (gegenüber 8 % im Vorjahr) oder sich einer verstärkten Bewertung durch ihre eigenen Kunden unterzogen zu haben (15 % gegenüber 10 %). Negative Publicity, die sich auf die Marke oder den Ruf des Unternehmens auswirkt, wurde von 14% der Befragten genannt (gegenüber 5% zuvor). Einer von acht Befragten (13%) gab an, einen Rückgang bei betriebswirtschaftlichen Indikatoren wie dem Aktienkurs erlebt zu haben (im Vergleich zu 5% im Vorjahr).

Definitionen

Cyber-Zwischenfall: Jedes Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder Informationen nicht beeinträchtigt. Dies könnte sowohl böswillige als auch nicht-böswillige Ereignisse umfassen.

Cyber-Schaden: Ein Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder Informationen erfolgreich beeinträchtigt und zu einem materiellen Verlust für das Unternehmen führt. Dies könnte sowohl böswillige als auch nicht böswillige Ereignisse umfassen.

Cyber-Readiness-Modell

Die Zahl der als Cyber-Experten definierten Unternehmen stieg erfreulicherweise an.

Große Firmen sind Vorreiter

Der Prozentsatz der Unternehmen, die sich in unserem Cyber Readiness-Modell als "Experten" qualifizieren, hat sich innerhalb eines Jahres fast verdoppelt – von 10% auf 18%. Umgekehrt ist die Zahl der Unternehmen, die in die Kategorie "Anfänger" fallen, von 74% auf 64% gesunken. Die Readiness-Werte waren im Vorjahr noch leicht gesunken, was damals darauf hindeutete, dass der Fortschritt zum Stillstand gekommen war.

Cyber-Readiness-Status

Die erstmalige Einbeziehung irischer Unternehmen hat dazu beigetragen, den Mittelwert anzuheben. Irische Firmen sind mit 24% an der Spitze der Readiness-Tabelle vertreten, die sich als Experten qualifizieren, da sie entweder über einen eigenen Cybersicherheits-Verantwortlichen oder ein engagiertes Team verfügen (89%).

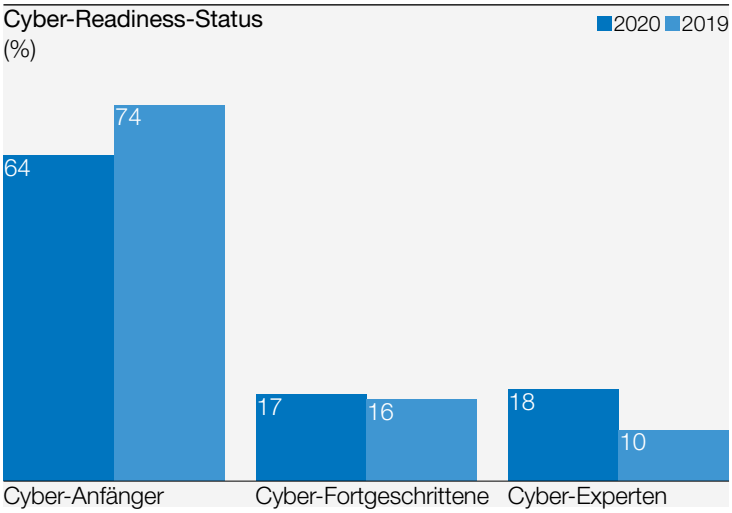
Dies mag die große Zahl globaler Finanz- und Technologieunternehmen widerspiegeln, die Irland als europäischen Hauptsitz ausgewählt haben, auch wenn die Gewichtung dieser Sektoren in dem Land nicht merklich vom Mittelwert abweicht.

Jedes Land hat jedoch zu dieser Verbesserung beigetragen. Frankreich, das in den beiden vorangegangenen Berichten noch im Hintertreffen lag, konnte seinen Anteil an Experten verdreifachen – von 6% auf 18% - vielleicht der Lohn für das außergewöhnliche Niveau der Cyber-bezogenen Ausgaben in den letzten zwei Jahren.

Die Größe ist nach wie vor entscheidend

Cyber-Readiness ist eindeutig ein Bereich, in dem es auf die Unternehmensgröße ankommt. Große Unternehmen verfügen über große Ressourcen. Es besteht ein klarer Zusammenhang zwischen den Beschäftigten im Bereich Sicherheit und dem Cyber-Readiness eines Unternehmens. Beispielsweise machen Unternehmen, die mehr als 50 Mitarbeiter in ihrem Sicherheitsteam beschäftigen, nur 11% der gesamten Befragten aus, stellen aber 19% der Cyber-Experten dar. Bei Unternehmen mit mehr als 1.000 Mitarbeitern verfügen 29% der Unternehmen über Sicherheitsteams dieser Größe.

Große Unternehmen geben für Cybersicherheit ein Vielfaches mehr aus als ihre kleineren Pendants. Während Kleine Unternehmen im vergangenen Jahr im Schnitt 11.818 € ausgaben, investierten Firmen mit 1.000 und mehr Angestellten durchschnittlich 7,27 Millionen €. Im Großen und Ganzen wird in Know-how investiert. Firmen, die als Experten eingestuft werden, gaben im vergangenen Jahr



durchschnittlich 3,8 Millionen € für Cybersicherheit aus; Firmen am unteren Ende der Skala gaben durchschnittlich 1,2 Millionen € aus.

Es ist daher interessant, dass mit mehr kleineren Unternehmen in diesem Jahr sich die Cyber-Readiness insgesamt dennoch verbessert hat. Dies ist weitgehend auf eine mindestens Verdoppelung der Zahl der kleinen, mittleren und großen Unternehmen zurückzuführen, die im Vergleich zum Vorjahr als Experten eingestuft wurden.

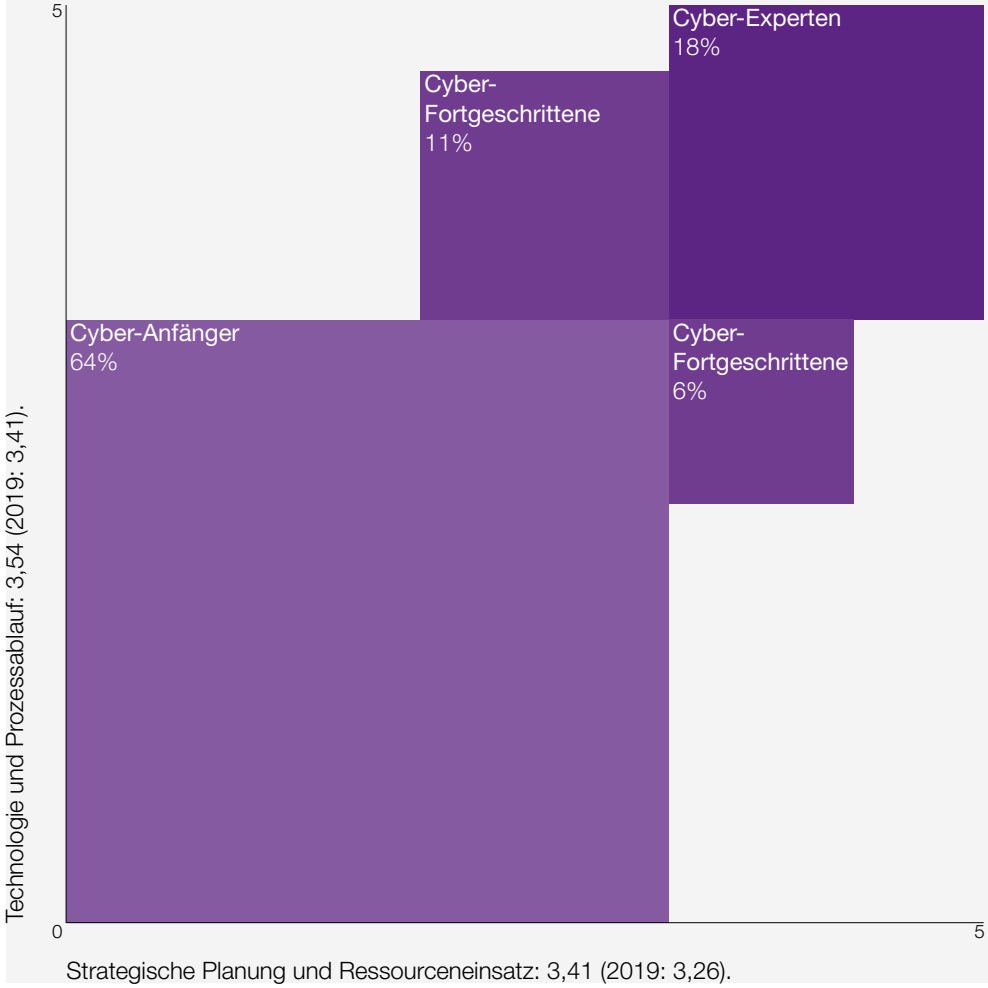
Es ist daher interessant, dass mit mehr befragten kleineren Unternehmen in diesem Jahr sich die Cyber-Readiness insgesamt dennoch verbessert hat. Dies ist weitgehend auf mindestens eine Verdoppelung der Zahl der kleinen, mittleren und großen Unternehmen zurückzuführen, die im Vergleich zum Vorjahr als Experten eingestuft wurden. Im Gegensatz dazu wurden fast vier von fünf Kleinstunternehmen mit einem bis neun Mitarbeitern (79%) als "Cyber-Anfänger" eingestuft. Bei allen Befragten stieg die Zahl derer, die angaben, ihre Firma habe "keine definierte Zuständigkeit" für die Cybersicherheit, von 16% auf 20% (fast die Hälfte der Kleinstunternehmen – 48% – hatten keine solche Zuständigkeit definiert). Der Anteil derer, die externe Dienstleister in Anspruch nahmen, blieb mit 19% konstant.

2x

Der Anteil der Unternehmen, die sich als Cyber-Experten qualifizieren, hat sich binnen eines Jahres fast verdoppelt.

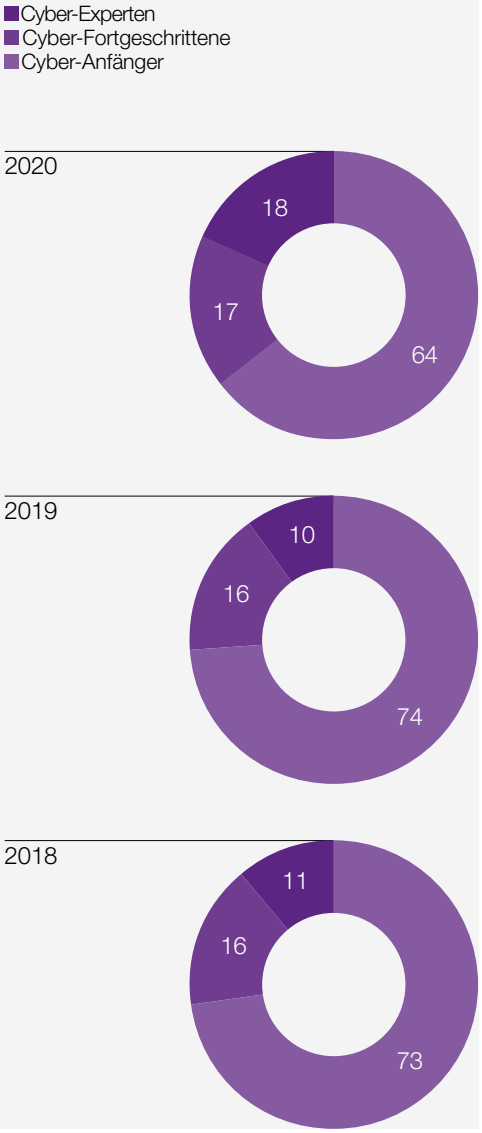
Wie das Modell aufgebaut ist

Unser Cyber-Readiness-Modell misst die Ausrichtung der Unternehmen anhand von vier Bereichen – strategische Planung und Ressourceneinsatz auf der einen Achse sowie Technologie und Prozessablauf auf der anderen. Unternehmen, die auf beiden Achsen vier von fünf Punkten erreichen, gelten als "Cyber-Experten". Diejenigen, die diese Punktzahl nur auf einer Achse erreichen, sind "Cyber-Fortgeschrittene". Unternehmen, die weder das eine noch das andere erreichen, gelten als "Cyber-Anfänger".



Cyber Readiness im Jahresvergleich

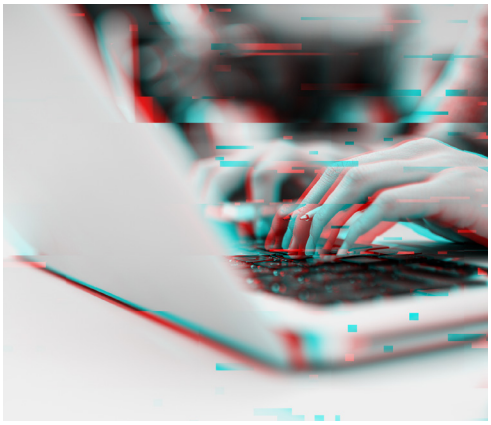
(%)



Was können Unternehmen von den Experten lernen?

Gute Grundlagen schaffen
Identifizieren Sie jedes Gerät in der Firma. Sichern Sie Daten außerhalb des Unternehmens. Und lernen Sie aus jedem Zwischenfall oder Schadenfall. Auch Experten werden nach einem Schadenfall eher bereit sein, ihre Strategie zu verbessern - durch regelmäßige Evaluierung der Sicherheit, die Einführung zusätzlicher Sicherheits- und Audit-Anforderungen und höhere Ausgaben für das Krisenmanagement.

Einem Regelwerk folgen
Es geht um umfassende Schutzmaßnahmen, die sicherstellen, dass alle virtuellen Türen und Fenster geschlossen sind. Ein Regelwerk, wie es vom US-amerikanischen National Institute of Standards and Technology (NIST) definiert wurde, der um fünf Forderungen herum aufgebaut ist - Identifizieren, Schützen, Aufspüren, Reagieren und Wiederherstellen – bietet eine nützliche Checkliste. Im Durchschnitt ergreifen die Experten in allen fünf Bereichen doppelt so viele Maßnahmen wie die Neulinge.



Keine falsche Sparsamkeit
Cyber-Experten wenden einen größeren Anteil ihres IT-Budgets für die Cyber-Sicherheit auf, und mehr von ihnen planen, die Ausgaben in allen Cyber-bezogenen Bereichen im kommenden Jahr zu erhöhen. Einfach ausgedrückt: Je mehr ein Unternehmen in die Cybersicherheit investiert, desto eher zählt es zu den Cyber-Experten.

In das Wissen investieren
Cyber-Anfänger erlitten wesentlich mehr Schäden durch erfolgreiche Phishing- und Malware-Angriffe. Regelmäßige Schulungen zur Sensibilisierung der gesamten Belegschaft sind unerlässlich. Dies ist nur zum Teil eine Frage der Ressourcen. Fast drei Viertel der Kleinstunternehmen, die als Experten eingestuft werden, beabsichtigen, der Einführung einer effektiven Mitarbeiterschulung im gesamten Unternehmen im kommenden Jahr Vorrang einzuräumen.

Das Management einbeziehen
Neun von zehn Experten sagen, dass "Cybersicherheit für die Geschäftsleitung/ den Vorstand höchste Priorität hat". Gerade einmal die Hälfte der Cyber-Anfänger ist in der Lage, dasselbe zu sagen. Was die Prioritäten für das kommende Jahr anbelangt, so erkennt nur ein Viertel der Cyber-Anfänger unter den Kleinstunternehmen die Notwendigkeit, das Engagement der Geschäftsführung oder des Vorstands in Bezug auf Richtlinien und Verfahren zur Cybersicherheit zu verstärken. Im Vergleich erkennen dies fast zwei Drittel der Experten der gleichen Unternehmensgröße.

Cyber-Resilienz aufbauen
Kein Unternehmen wird jemals vollkommen sicher sein. Aber alle können Widerstandsfähigkeit aufbauen, indem sie sich auf einen Cyber-Angriff vorbereiten, Testläufe durchführen und im Ernstfall in der Lage sind, schnell und effektiv zu reagieren. Eine eigenständige Cyber-Versicherungspolice trägt zum Aufbau dieser Resilienz bei, indem sie den Unternehmen nicht nur die Gewissheit einer finanziellen Deckung gibt, sondern auch die Fähigkeit, auf spezielles externes Fachwissen zurückzugreifen - bei Risikobewertungen, Krisenmanagement und Mitarbeiterschulungen.

Wie kleinere Firmen erfolgreich waren

Wie die Zahlen in der Tabelle zeigen, ist auch die Zahl der Klein- und Kleinstunternehmen, die als Experten eingestuft werden, deutlich gestiegen. Wer waren sie und was haben sie richtig gemacht? Jedes sechste von ihnen (16% Experten) waren digital versierte Unternehmen aus den Bereichen Technologie, Medien und Telekommunikation (TMT), während der Einzel-/Großhandel und das Baugewerbe ebenfalls gut vertreten waren (mit 11% bzw. 10%). Die meisten scheinen ihren Expertenstatus erreicht zu haben, weil sie die Cybersicherheit ernst nehmen. Die Analyse zeigt, dass sie alle folgende drei Maßnahmen ergriffen haben:

- Aktive Schulung des Cyberbewusstseins;
- Konsistener Einsatz von Viren-/Anti-Malware-Systeme im gesamten Unternehmen;
- Entscheidungen werden auf Grundlage klar definierter Unternehmensanforderungen/ Cyber-Sicherheit-Spielräumen getroffen.

Die am stärksten aufgestellten Branchen

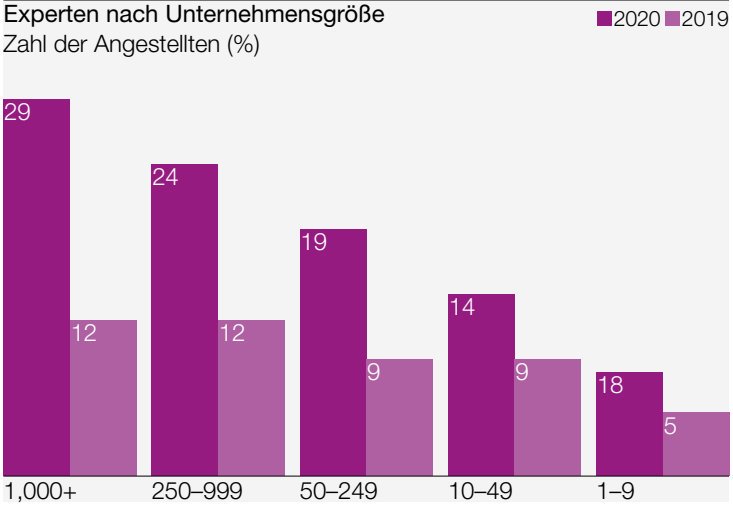
Insgesamt befanden sich die Unternehmen aus den Bereichen Finanzdienstleistungen und TMT erneut unter den ersten drei (24% bzw. 23% mit Experten-Status), aber in diesem Jahr kam das produzierende Gewerbe (24%) neu hinzu. Die Erklärung könnte darin liegen, dass in dieser Branche Kleinstunternehmen eine stärkere Rolle spielen als in den meisten anderen. Die Lebensmittel-Branche stellt das Schlusslicht dar, da hier nur 7% der Unternehmen als Experten eingestuft wurden.

Haben die Experten besser abgeschnitten?

Im Allgemeinen schnitten die gut vorbereiteten Firmen wesentlich besser ab als die Cyber-Anfänger. Letztere hatten eine dreimal höhere Wahrscheinlichkeit, einen Schadenfall zu erleiden als die Experten, mit einem Median von 30 pro Unternehmen gegenüber neun bei den Experten.

Experten nach Unternehmensgröße

Experten nach Unternehmensgröße
Zahl der Angestellten (%)



Das Übergewicht von Großunternehmen und Konzernen (mit über 1.000 Beschäftigten) unter den Experten könnte ihre höhere Schadenquote erklären, da größere Unternehmen mehr Angriffsfläche bieten, Cyberkriminellen größere Erlöse ermöglichen und wahrscheinlich besser in der Lage sind, Schäden zu erkennen. Zwei von fünf großen Unternehmen gelten als Experten, während 60% der Firmen mit weniger als 100 Mitarbeitern als Neulinge gelten.

Eines der auffälligeren Ergebnisse ist, dass fast jeder fünfte (19%) der Cyber-Anfänger, die von einem Cyber-Vorfall betroffen waren, ein Lösegeld zahlen mussten. Kleinere, anfälligere Firmen stehen wahrscheinlich in der Schusslinie, und die weniger gut darauf vorbereiteten unter ihnen zahlen eindeutig den Preis dafür.

Die Hiscox Sicht

Wir sehen zwei häufige Arten von Lösegeldangriffen: Gezielte Attacken – eher auf größere Organisationen ausgerichtet (so genannte "Big Game Ransomware"), wo eine Hackergruppe mit hoch personalisierten Phishing-Betrügereien gezielt Schlüsselpersonen ins Visier nimmt Massenscanning - Hacker suchen nach den wesentlichen Schwachstellen in Servern, die im Internet zugänglich sind (in jüngster Zeit Fernzugriff und VPN-Server). In diesen Fällen sind die Angriffe meist unterschiedslos, und die Angreifer infizieren jedes Unternehmen, das sie für verwundbar halten.

Gestiegene Resilienz

Eine Vielzahl von Indikatoren deuten darauf hin, dass der Großteil der Unternehmen die Cyber-Gefahr ernster als je zuvor nehmen.

Gestiegene Ausgaben

Da sind zunächst gestiegenen Ausgaben für Cybersicherheit. Der Report zeigt einen sehr starken und breiten Anstieg im vergangenen Jahr - mit einem durchschnittlichen Ausgabenvolumen in unserer Studiengruppe von 1,8 Millionen € gegenüber 1,3 Millionen € im Vorjahr. Das ist ein Anstieg von 39%. Er spiegelt sowohl eine Erhöhung der IT-Gesamtbudgets als auch einen Anstieg des Anteils der Cyber-Sicherheits-Ausgaben um 30 % Prozentpunkte (von 9,9 % auf 12,9 %) wider. Große Konzerne haben hier die Führung übernommen.

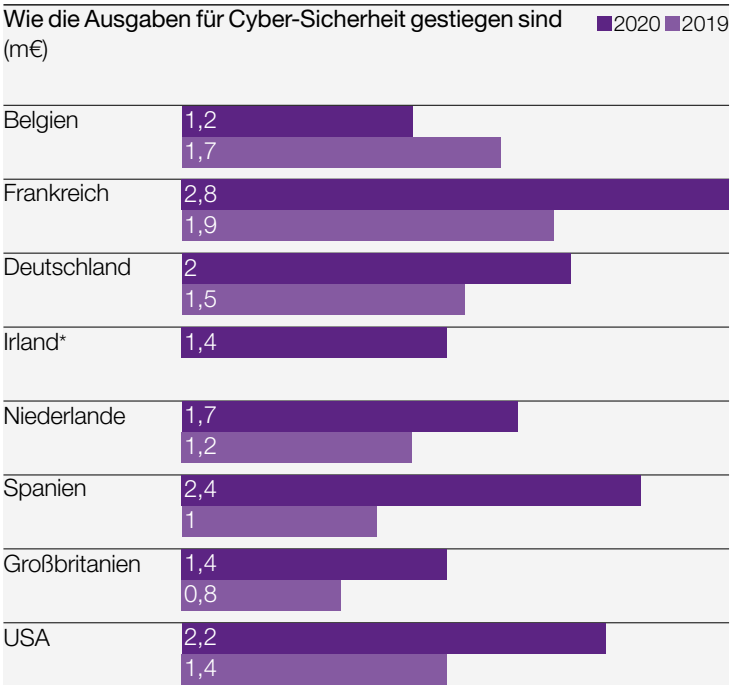
Französische Firmen machten erneut die größten Ausgaben und erhöhten ihre Cyberbudgets von durchschnittlich 1,9 Millionen € auf 2,8 Millionen €. Knapp dahinter folgten spanische und US-amerikanische Firmen mit 2,4 Millionen € bzw. 2,2 Millionen €. Das Vereinigte Königreich, in früheren Studien ein Nachzügler, begann aufzuholen – mit durchschnittlichen Ausgaben für Cyber in Höhe von 1,4 Millionen € gegenüber knapp 0,8 Millionen € im Vorjahr.

Etwas mehr als drei Viertel der Befragten machten konkrete Aussagen zu ihren Ausgaben für Cybersicherheit. Wenn man davon ausgeht, dass diese repräsentativ für die gesamte Studiengruppe waren, beliefen sich die Gesamtausgaben für Cybersicherheit im vergangenen Jahr auf erstaunliche 10,4 Millionen €. Im Vergleich dazu waren es vor einem Jahr bei einer um 3% kleineren Stichprobe 7,2 Millionen €.

Wie die Ausgaben für Cyber-Sicherheit gestiegen sind

Ein durchschnittliches Kleinstunternehmen mit weniger als zehn Mitarbeitern gab rund 11.800 € für Cybersicherheit aus. Ein durchschnittlicher Konzern gab 7,3 Millionen € aus.

Fast drei Viertel der Unternehmen (72%) beabsichtigen, ihre Cyber-Ausgaben im kommenden Jahr um 5% oder mehr zu erhöhen. Das ist ein Anstieg gegenüber zwei Dritteln (67%) vor einem Jahr. Im Durchschnitt planen die Cyber-Experten, ihre Budgets um etwas mehr als 15% zu erhöhen, während die Cyber-Neulinge ihr Budget um knapp 12% erhöhen wollen. Dies deutet darauf hin, dass sich die Kluft zwischen den am stärksten und den am schwächsten aufgestellten Unternehmen vergrößern wird.



Sind hohe Ausgaben gleichbedeutend mit hoher Cyber-Readiness?

Die Antwort auf diese Frage ist nicht eindeutig. Auf der einen Seite war es bei Firmen, die zweistellige Prozentsätze ihres IT-Budgets ausgaben, weniger wahrscheinlich, dass es zu einem Cyber-Vorfall oder -Schadenfall kam als bei Firmen, die weniger als 5% ausgaben. Die Firmen mit hohen Cyber-Ausgaben – bei denen es sich in der Regel auch um die größeren Unternehmen handelte – hatten jedoch auch höhere Durchschnittskosten für Angriffe zu tragen. Größe führt zu mehr Kunden, aber auch zu höheren Benachrichtigungskosten und höheren Lösegeldforderungen.

*Daten nur für 2020 verfügbar.

Ermittlung der Ausgabenprioritäten im Jahr 2020
(%)

	Cyber-Experten	Cyber-Anfänger
Erreichen oder Aufrechterhalten der Einhaltung gesetzlicher Vorschriften	82	44
Behebung bestehender Bedrohungen oder Schwachstellen	81	44
Einhaltung der Sicherheitsanforderungen, die von Geschäftspartnern an uns gestellt werden	80	42
Sicherstellen, dass Geschäftspartner oder Dritte unsere Sicherheitsanforderungen erfüllen	79	40
Verbesserung der Sicherheit kundenorientierter Dienste oder Apps	78	40

In welche Bereiche lenken die Unternehmen ihre Ausgaben? In den letzten drei Jahren hat sich eindeutig der Schwerpunkt verlagert. Der Anteil der Befragten, die planen, ihre Ausgaben für neue Cyber-Sicherheitstechnologien zu erhöhen, ist in dieser Zeit allmählich von 57% auf 46% gesunken, während die Zahl derer, die mehr in die Sensibilisierung der Mitarbeiter investieren wollen, von 34% auf 40% gestiegen ist. Mehr als ein Drittel (35%) plant, die Planung für die Cybersicherheit zu erhöhen, gegenüber 26% vor zwei Jahren.

Ermittlung der Ausgabenprioritäten im Jahr 2020

Gestiegenes Bewusstsein

Wie im vergangenen Jahr fragten wir die Befragten nach ihren obersten Ausgabenprioritäten für das kommende Jahr, wobei wir uns auf das Rahmenwerk für Cybersicherheit des amerikanischen National Institute of Standards and Technology (NIST) stützten. Betrachtet man die letzten drei Jahre, so hat sich an den als am dringlichsten erachteten Initiativen wenig geändert. Aber die Zahl der Firmen, die diese Punkte abgearbeitet haben, ist von Jahr zu Jahr gestiegen, was auf ein zunehmendes Bewusstsein für die Notwendigkeit eines breit angelegten und aktiven Ansatzes im Bereich der Cybersicherheit hindeutet.

Steigende Ausgaben in jeder NIST-Kategorie

Die Befürwortung solcher Initiativen nimmt sowohl mit der Größe des Unternehmens als auch mit der höherer Cyber-Readiness zu (siehe Tabelle unten). Die Experten in unserer Stichprobe haben eindeutig längere To-Do-Listen. Nicht weniger als vier von fünf erwähnten die oben genannten Prioritäten für das kommende Jahr. Sie legten wahrscheinlich auch mehr Gewicht auf die "Durchführung von Cyber-Sicherheitsbeurteilungen", und sie waren deutlich schärfer auf die "Sicherung des Internet der Dinge innerhalb des Unternehmens" bedacht.

Eine neue Dringlichkeit

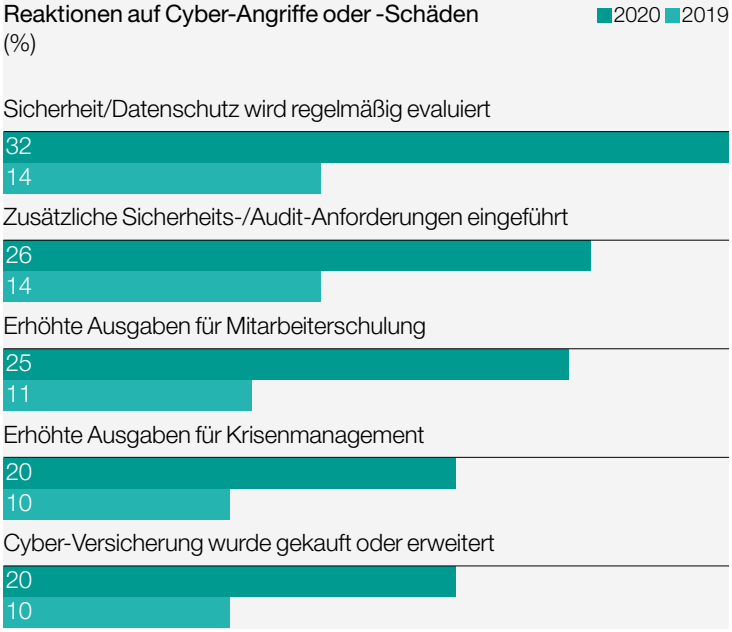
Es gibt einen weiteren Indikator für eine neue Entschlossenheit, die Cyber-Bedrohung zu bekämpfen: Die Art und Weise, wie Unternehmen in den letzten 12 Monaten entweder auf einen Cyber-Zwischenfall oder auf einen Cyber-Schaden reagiert haben. Plötzlich handeln Unternehmen mit einer neuen Dringlichkeit. In der Regel geben etwa doppelt so viele Unternehmen an, zusätzliche Maßnahmen zur Bekämpfung der Hacker ergriffen zu haben wie im letzten Jahr.

Reaktionen auf Cyber-Angriffe oder -Schäden

Steigende Ausgaben in jeder NIST-Kategorie
(%)

	2020	2019	2018
Identifizieren	50	46	44
Schützen	50	45	44
Erkennen	50	47	45
Reagieren	44	39	39
Wiederherstellen	46	43	41

Reaktionen auf Cyber-Angriffe oder -Schäden
(%)



Experten sind in Sachen Cyber-Versicherung voraus

Der Anteil der Befragten, die angeben, dass sie eine Cyber-Versicherung aufgrund eines früheren Cyber-Vorfalls oder -Schadens (nicht zwingend im vergangenen Jahr) abgeschlossen haben, hat sich in den letzten drei Umfragen kontinuierlich von 9% auf 29% erhöht.

In diesem Jahr haben wir den Fragebogen dahingehend geändert, dass die Teilnehmer nach einer "eigenständigen" Cyber-Police befragt wurden (im Gegensatz zum Cyber-Schutz im Rahmen einer allgemeineren Police). Etwas mehr als ein Viertel der Firmen (26%) gaben an, dass sie eine eigenständige Cyber-Police haben, und weitere 18% gaben an, dass sie planen, entweder eine eigenständige Deckung zu kaufen oder sie als Deckung in ihre Policen aufzunehmen.

Haben Sie eine Cyber-Versicherung?

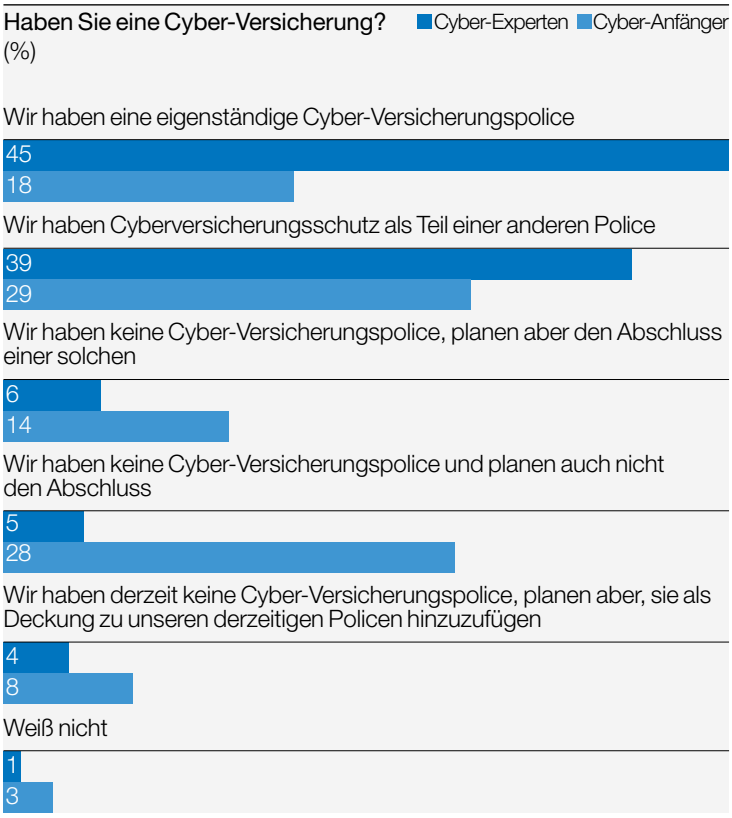
Dies ist ein Bereich, in dem die Experten eindeutig die Nase vorn haben. Fast die Hälfte (45%) gibt an, eine eigenständige Cyber-Police zu haben, und mehr als drei Viertel (70%) beabsichtigen, entweder eine Cyber-Deckung zu erwerben oder sie als Zusatzdeckung in ihre Police aufzunehmen.

Der Abschluss von eigenständigen Cyberversicherungen steigt mit der Größe der Unternehmen in unserer Umfrage stetig an – von nur 12% bei Kleinstunternehmen auf 42% auf Konzerngröße. In jeder Kategorie, mit Ausnahme der allergrößten, verlassen sich mehr Firmen auf eine andere, allgemeinere Police (die sie im Falle eines schwerwiegenden Schadenfalls absichert oder auch nicht).

Die Einführung eigenständiger Cyber-Strategien ist von Land zu Land sehr unterschiedlich. Irland führt die Liste an, wobei 38% der Unternehmen angeben, dass sie über eine spezielle Cyber-Deckung verfügen. Knapp dahinter folgen die USA (33%) und Belgien (30%). Großbritannien (22%) und Frankreich (23%) stehen am Ende der Liste.

Die Hiscox Sicht

Als Cyber-Versicherer versteht es sich von selbst, dass wir eine eigenständige Cyber-Versicherung empfehlen würden. Wichtig ist, dass die eigenständige Cyber-Versicherung dazu dient, Unternehmen nach einem Cyber-Angriff wieder ins Geschäft zurückzubringen. Die Cyber-Versicherung bietet eine Reihe von Dienstleistungen (IT-Forensik, Krisenkommunikation, Rechtsberatung und, falls erforderlich, Kreditkartenüberwachung), um Unternehmen dabei zu helfen, schnell zur Normalität zurückzukehren.



Forschungs-Methodologie

Hiscox beauftragte Forrester Consulting mit der Bewertung der Cyber-Readiness von Organisationen. Insgesamt wurden 5.569 Fachleute kontaktiert, die für die Cyber-Sicherheitsstrategie ihrer Organisation verantwortlich sind (jeweils über 1.000 aus Großbritannien, den USA und Deutschland; jeweils mehr als 500 aus Belgien, Frankreich, Spanien und den Niederlanden; und über 300 aus der Republik Irland). Die Teilnehmer beantworteten die Online-Umfrage zwischen dem 24. Dezember 2019 und dem 3. Februar 2020.

Der Anteil kleiner Unternehmen mit weniger als 250 Beschäftigten erhöhte sich von 56% auf 60%. Firmen mit bis zu neun Beschäftigten machen nun 29% der Studiengruppe aus (2019: 20%). Der Anteil von Einzelunternehmern liegt bei 10% (2019: 5%). Großunternehmen (mit 250 bis 999 Beschäftigten) und Großkonzerne mit mehr als 1.000 Beschäftigten machen zusammen weiterhin 40% der Befragten aus.

In diesem Jahr wurde die Anzahl der Zwischenfälle, Schäden und Kosten vor allem anhand des Median- anstelle des Mittelwertes erfasst. Die Vorjahreszahlen wurden in gleicher Weise angepasst. Angesichts der extremen Unterschiede in den zugrundeliegenden Zahlen der kleinsten und der größten Unternehmen ergibt sich dadurch eine genauere Darstellung der Ergebnisse.

Die vollständige Zusammensetzung der Befragten ist unten dargestellt.

Entscheidungsebene der Befragten	%
Vorstands-Ebene/Gründer	31
Vizepräsident	21
Geschäftsführer	39
Manager	9

Größe des Unternehmens	%
1,000+	25
250–999	15
50–249	15
10–49	15
1–9	29

Branchen	%
Unternehmensdienstleistungen	7
Energie	4
Baugewerbe	8
Finanzdienstleistungen	9
Lebensmittel	4
Regierung und gemeinnützige Organisationen	7
Produzierendes Gewerbe	8
Pharma und Gesundheitswesen	9
Freiberufliche Dienstleistungen	9
Immobilien	4
Einzel- und Großhandel	9
Technologie, Medien, Telekommunikation	16
Transport und Distribution	4
Reisen und Freizeit	4

Bereiche, in denen die Befragten arbeiten	%
Vorstand/Geschäftsführung	13
eCommerce	2
Finanzen	8
Beratung	3
HR	4
IT/Technik	21
Marketing/Kommunikation	3
Operations	10
Eigentümer	21
Einkauf	3
Produkt-Management	4
Risiko-Management	3
Vertrieb	5

Hiscox SA

Niederlassung für Deutschland
Arnulfstr. 31
80636 München

+49 (0)89 54 58 01 100
hiscox.info@hiscox.de

hiscox.de/cyber-readiness-report-2020

20647 6/20