Umgang mit Cyberrisiken

20. September 2016

Ein Bericht von Lloyd's

LLOYD'S

Inhalt

Teil 1
Zusammenfassung

1.1 Zusammenfassung

Unabhängig von Größe und Standort sind heute praktisch alle Unternehmen auf Digitaltechnik angewiesen. Sie hilft Unternehmen, effizienter zu werden, Kosten zu senken und neue Märkte zu erschließen, macht sie aber auch anfällig für Cyberangriffe. In den vergangenen zwei Jahren hat eine Reihe spektakulärer Cybervorfälle – bei denen vielfach personenbezogene Daten von Kunden in falsche Hände geraten sind – das Thema Cybersicherheit in den Vordergrund gerückt.

Zusätzliche Dringlichkeit gewinnt das Thema durch das Inkrafttreten der Datenschutz-Grundverordnung der Europäischen Union im Jahr 2018, die hohe Anforderungen an alle Unternehmen stellt, die Daten von europäischen Verbrauchern verarbeiten.

Lloyd's – das weltweite Zentrum für Cyberversicherung – hat mithilfe der vorliegenden Umfrage ermittelt, wie europäische Unternehmen mit dem Thema Cybersicherheit umgehen und wie sie sich auf die Datenschutz-Grundverordnung vorbereiten.

Hierbei wurden 346 hochrangige Entscheidungsträger in Großunternehmen (mindestens 250 Mio. € Umsatz) aus ganz Europa befragt. Die Befragten bekleideten Funktionen wie Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operating Officer (COO), Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Risk Officer (CRO) und General Counsel.

Die meisten großen Unternehmen in Europa haben in den vergangenen fünf Jahren eine Datenschutzverletzung erlitten, befürchten allerdings keinen Wiederholungsfall.

- 92 % der Befragten gaben an, es habe in den vergangenen fünf Jahren eine Datenschutzverletzung in ihrem Unternehmen gegeben. Aber nur 42 % befürchteten, dass es in Zukunft erneut zu Datenschutzproblemen kommen kann.

Im vergangenen Jahr haben Cyberrisiken die Prioritätenlisten der Führungskreise erobert. Wenn es um Cybersicherheit geht, trifft heutzutage der CEO die strategischen Entscheidungen, nicht mehr der CIO.

- Pläne zur Vorbeugung und Schadensbegrenzung im Fall von Datenschutzverletzungen sind inzwischen bei der Mehrheit der Befragten (54 %) Sache des CEOs. Entsprechend trifft nur noch in 10 % der Fälle der CIO die relevanten Entscheidungen. Dies ist das Resultat einer Reihe medienträchtiger Cybervorfälle in verschiedenen Teilen der Welt, die zum Teil massive Auswirkungen auf Unternehmensergebnisse und Aktienkurse hatten und in einigen Fällen sogar zu Ablösungen an der Unternehmensspitze geführt haben.

Viele wissen, dass die europäische Datenschutz-Grundverordnung kommt, sind sich aber nicht der Tragweite bewusst – mit unter Umständen ernsthaften Konsequenzen.

- 97 % der Befragten hatten von der Datenschutz-Grundverordnung gehört, aber nur 7 % wussten „sehr viel" darüber. 57 % sagten, sie wüssten „wenig" bzw. „gar nichts" über die neue Verordnung, trotz der ernsten finanziellen und rechtlichen Konsequenzen bei Nichteinhaltung ihrer Bestimmungen.

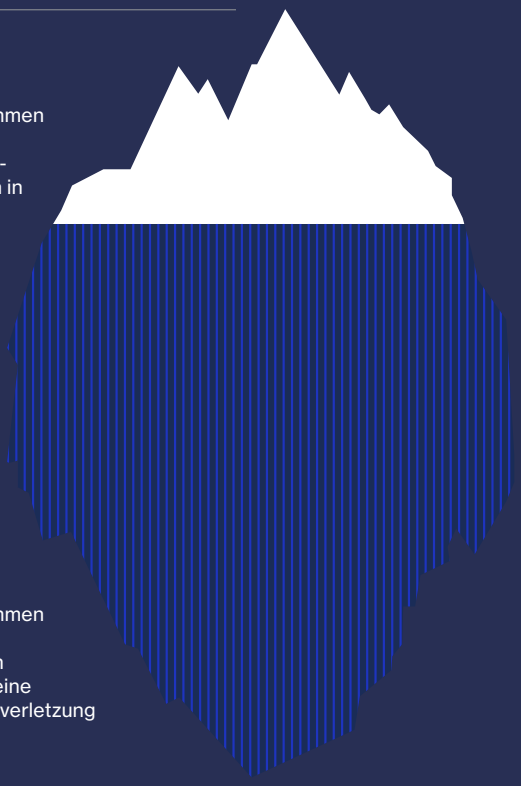
- Mehr als die Hälfte der befragten Unternehmen war sich darüber im Klaren, dass die Datenschutz-Grundverordnung für sie Auswirkungen in Form von behördlichen Untersuchungen (64 %), finanziellen Sanktionen (58 %), Wertverlust der Aktien (57 %) und Imageschäden (52 %) haben kann, aber nur 13 % hielten es für möglich, dass sie Kunden verlieren könnten.

1.2 Fazit

Die europäischen Unternehmen sind einer sich ständig weiterentwickelnden Umgebung von Cyberbedrohungen ausgesetzt. Die Einführung der Datenschutz-Grundverordnung wird die Aufmerksamkeit auf den Aspekt der Datensicherheit in Unternehmen lenken, denn Behörden, Aktionäre und Kunden werden auf ihrer Grundlage höhere Datenschutzstandards von den Unternehmen verlangen. Professionelle Partnerschaften mit Rechtsanwälten, Experten für Cybersicherheit und Spezialversicherern helfen Unternehmen, ihre Risiken besser einzuschätzen und sie im Interesse der Bilanzsicherung zu begrenzen.

42%

der Unternehmen befürchten Datenschutz-verletzungen in der Zukunft



92%

der Unternehmen haben in den vergangenen fünf Jahren eine Datenschutzverletzung erlebt

97%

der Unternehmen haben von der neuen EU-Datenschutz-Grundverordnung gehört

57%

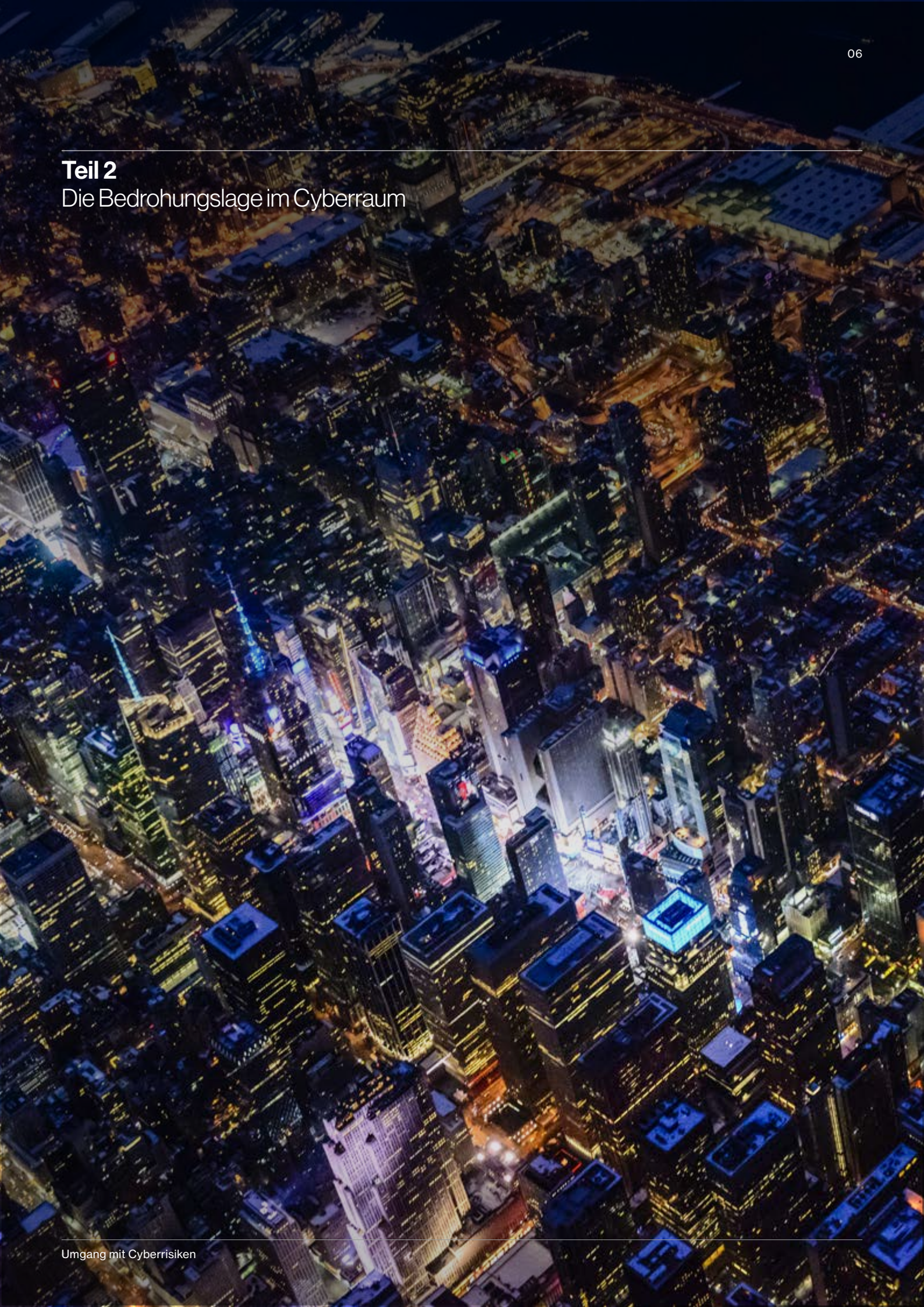
der Unternehmen wissen wenig oder nichts über die neue EU-Datenschutz-Grundverordnung

Was Cyberversicherung leisten kann

- Laut der vorliegenden Umfrage verfügen 73 % der Unternehmensführer nur über begrenztes Wissen über Cyberversicherung und 50 % wissen gar nicht, dass die Risiken von Datenschutzverletzungen versicherbar sind.
- Die Cyberversicherung erbringt nach einem Cyberangriff nicht nur finanzielle Leistung, sondern bietet auch Expertenberatung zur Erhöhung der Sicherheit und konkrete Unterstützung im Krisenfall.
- Von der Zusammenarbeit mit kompetenten Spezial-versicherern profitiert die Sicherheitsstrategie des Unternehmens. Der Versicherer kann Unternehmen helfen, Risiken und Schwachstellen zu erkennen, um das Risiko einer Datenschutzverletzung von vornherein zu reduzieren.
- All dies dient der Absicherung der Bilanz des Einzelunternehmens und der branchenweiten Erhöhung der Standards für Cybersicherheit und Risikominderung.

Weitere Informationen: www.lloyds.com/cyber

Teil 2
Die Bedrohungslage im Cyberraum



2.1 Cyberrisiken auf dem Vormarsch

Unabhängig von Größe und Standort sind heute praktisch alle Unternehmen auf Digitaltechnik angewiesen. Einzelhändler, Finanzdienstleister und Anbieter von schnelldrehenden Konsumgütern verwenden Digitaltechnik zur Abwicklung ihrer Geschäfte, zur Kontrolle ihrer Bestände, zur Produktentwicklung, zur Kommunikation und zur Speicherung von Kundendaten.

Dabei hilft diese Technik Unternehmen, effizienter zu werden, Kosten zu senken und neue Märkte zu erschließen, macht sie aber auch anfällig für Cyberangriffe.

Aus diesem Grund ist Cybersicherheit ein wichtiges Thema für die Wirtschaft geworden. Cyberrisiken haben als Bedrohung, die jedes Unternehmen bewerten, vermindern und systematisch managen muss, inzwischen denselben Rang wie die klassischen Risiken Sachschaden, Terrorismus und Naturkatastrophen.

Das gesteigerte Bewusstsein der Wirtschaft für Cyberrisiken ist das Resultat einiger aufsehenerregender Vorkommnisse in den vergangenen Jahren in verschiedenen Teilen der Welt. Die jüngste spektakuläre Cyberattacke in Großbritannien richtete sich im Herbst 2015 gegen den Telekommunikationsanbieter TalkTalk. In anderen Ländern Europas gab es u. a. Angriffe auf den französischen Fernsehsender TV5 Monde, das schwedische Flugsicherungssystem, auf norwegische Mineralöl- und Energieunternehmen sowie ein deutsches Stahlwerk. In den USA gelangen Cybervorfälle seit 2014 immer wieder in die Schlagzeilen, darunter Angriffe auf Sony, Target, Home Depot und Experian.

Dementsprechend hat der Lloyd's-Markt, der vor 10 Jahren die erste Police für Cyberrisiken auf den Markt gebracht hat, ein schnelles Wachstum des Cyberversicherungsmarkts beobachtet. Inzwischen bieten 65 Versicherer des Lloyd's-Markts Cyber-versicherungen mit einer Gesamtkapazität von 300 Mio. £ an. Ihre Geschäfte repräsentieren ein Viertel des internationalen Cyberversicherungsmarkts und machen Lloyd's zum weltweiten Zentrum für Cyberversicherung.

Der vorliegende Bericht basiert auf einer Umfrage unter 346 hochrangigen Entscheidungsträgern großer europäischer Unternehmen. Er analysiert, wie Wirtschaftslenker mit dem Thema Cybersicherheit umgehen und welche Maßnahmen sie ergreifen, damit ihre Unternehmen für den Fall eines Cyberangriffs gerüstet sind.

Untersucht wurde außerdem, wie gut die europäischen Unternehmen auf die Einführung der Datenschutz-Grundverordnung der EU vorbereitet sind, die 2018 in Kraft tritt. Diese neue Verordnung wird die geltenden Bestimmungen und Verantwortlichkeiten für den Umgang von Unternehmen mit Verbraucherdaten und deren Schutz deutlich verschärfen. Mit ihr wird eine Reihe von Bestimmungen für Unternehmen eingeführt, die von einer Datenschutzverletzung betroffen sind, u. a. die Verpflichtung zur Meldung innerhalb von 72 Stunden, unter Androhung erheblicher Bußgelder bei Nichteinhaltung.

Der vorliegende Bericht konzentriert sich auf eine Art von Cybervorfällen: Verletzungen des Datenschutzes, denn der Schutz vertraulicher Daten – insbesondere der Finanz- und Gesundheitsdaten von Kunden – hat für die meisten Unternehmen oberste Priorität. Digitale Informationen sind ihr wichtigstes Betriebsmittel und daher die Zielscheibe der meisten Cyberangriffe.

2.2 Datenschutzverletzungen

Wie groß ist das Problem von Datenschutzverletzungen für europäische Unternehmen aktuell? Um das Ausmaß des Problems zu quantifizieren, wurden die Teilnehmer der Umfrage nach Datenschutzverletzungen in ihrem Unternehmen gefragt.

92% der Befragten gaben an, dass es in den vergangenen fünf Jahren eine Datenschutzverletzung gegeben habe, 3% gaben an, es habe „beinahe“ eine Datenschutzverletzung gegeben. Lediglich 5% sagten aus, es habe keine Datenschutzverletzung stattgefunden bzw. es sei keine Datenschutzverletzung bekannt.

Welche der folgenden Aussagen beschreibt die Erfahrungen Ihres Unternehmens mit Datenschutzverletzungen in den vergangenen 5 Jahren am besten:

Basis: Befragte insgesamt (346): Vereinigtes Königreich (100) Frankreich (31) Deutschland (34) Italien (30) Spanien (30) Niederlande (31) Norwegen (30) Dänemark (30)

2.3 Interne und externe Bedrohungen

Datenschutzverletzungen können sich aus ganz unterschiedlichen Cyberrisiken ergeben, von unabsichtlichen und versehentlichen Sicherheitslücken bis zu minutiös geplanten und bösartigen Angriffen. Die Umfrage ermittelte, welche Bedrohungen den Unternehmen am meisten Sorge bereiten.

Die Cyberbedrohungen wurden als „intern“ oder „extern“ klassifiziert. Interne Bedrohungen haben in der Regel ihren Ursprung im Unternehmen selbst, beispielsweise durch den Verlust oder Diebstahl von Daten oder Hardware oder durch mutwillige Weitergabe vertraulicher Daten durch eigene Mitarbeiter. Externe Bedrohungen sind meist technisch anspruchsvoll und umfassen Phänomene wie Hacking, Phishing, Ransomware und Malware (siehe nachstehendes Glossar).

Der Befragung zufolge empfinden die meisten Unternehmen externe Bedrohungen als gravierender als interne Bedrohungen. Unter den internen Bedrohungen wurde von 42 % der Befragten das technikferne Risiko des Verlusts von Dokumenten in Papierform als eine der größten Befürchtungen angegeben. Ebenso viele nannten die vorsätzliche Datenschutzverletzung durch Insider als eine ernstzunehmende Bedrohung.

Die am meisten gefürchtete externe Bedrohung sind Hackerangriffe. Die Hälfte (51 %) der befragten Unternehmen befürchteten einen Hackerangriff zwecks wirtschaftlicher Übervorteilung, während 46 % politische Gründe als denkbare Motivation für einen Hackerangriff angaben. 41 % nannten einen Hackerangriff durch einen Konkurrenten als ernste Gefahr.

Angesichts der vielbeachteten Datenschutzzwischenfälle in jüngerer Vergangenheit verwundert es nicht, dass Hacking als größte Bedrohung wahrgenommen wird. TalkTalk, Sony und Home Depot, um nur drei zu nennen, waren in der jüngeren Vergangenheit Zielscheibe von Cyberattacken. Auch wenn die eigentliche Motivation solcher Vorkommnisse häufig im Dunkeln liegt, können bei Angriffen dieser Art grundsätzlich Kundendaten gestohlen und an den Meistbietenden weiterverkauft werden.

Auch politische Motive kommen infrage, vor allem in geopolitisch umstrittenen Sektoren wie Energie und natürliche Ressourcen. Immer häufiger werden einzelne Organisationen von politisch motivierten Hackerkreisen angegriffen. Auch wenn das Ausmaß von Industriespionage schwierig zu quantifizieren ist, legt der dritte Rang für Hackerangriffe durch Konkurrenten nahe, dass Wirtschaftsführer hierin eine ernstzunehmende Gefahr sehen.

Glossar der Cyberbedrohungen

- Hacking – gezielte Suche nach und Ausnutzung von Schwachstellen in Computersystemen oder Netzwerken, typischerweise zur Erlangung finanzieller Vorteile.
- Phishing – Versuch, an vertrauliche Informationen heranzukommen, indem sich der Angreifer in einer E-Mail als vertrauenswürdige Person oder Organisation ausgibt.
- Whaling – ein Phishing-Versuch, bei dem sich der Angreifer als Autoritätsperson, häufig als Geschäftsführer, ausgibt.
- Malware – (Schadsoftware) bezeichnet alle Arten von Software, die dazu dient, den Rechnerbetrieb zu stören, vertrauliche Informationen zu sammeln oder Zugang zu privaten Computersystemen zu erlangen.
- Ransomware – (Erpressungstrojaner) ist Schadsoftware, welche die Computerfunktion stört und zu deren Wiederherstellung eine „Lösegeldzahlung“ fordert.

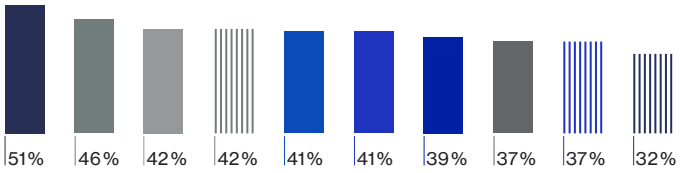
51 %

sind besorgt über die Möglichkeit eines finanziell motivierten Hackerangriffs

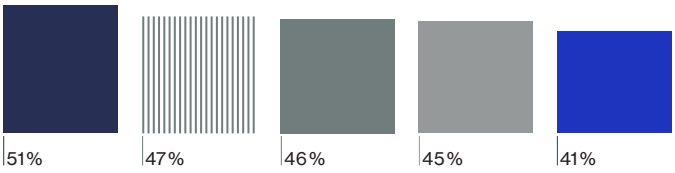
2.3 Interne und externe Bedrohungen

- Hacking – gewinnorientiert
- Hacking – durch Konkurrenten
- Hacking – politisch motiviert
- Menschliches Versagen / ungewollte Offenlegung
- Phishing
- Verloren gegangene, ausrangierte oder gestohlene Hardware
- Ransomware
- Malware
- Physischer Verlust von Unterlagen in Papierform oder nicht elektronischen Geräten
- Vorsätzliche Weitergabe von Daten durch Insider

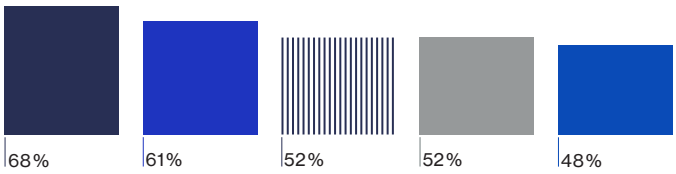
Gesamt



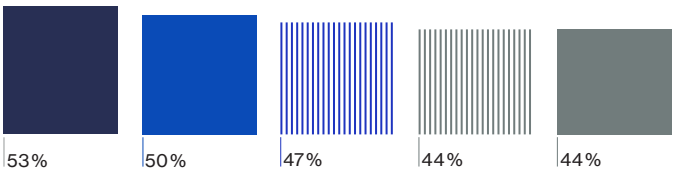
Vereinigtes Königreich



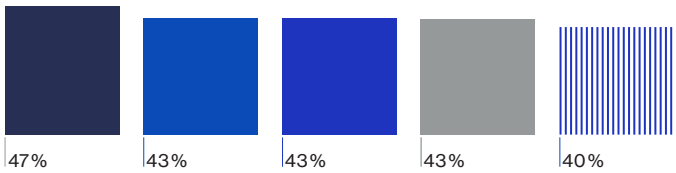
Frankreich



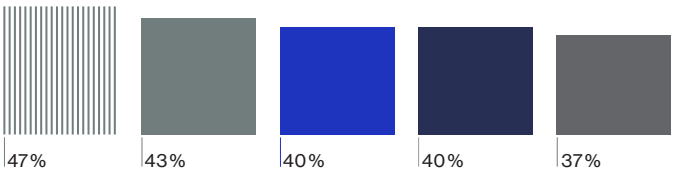
Deutschland



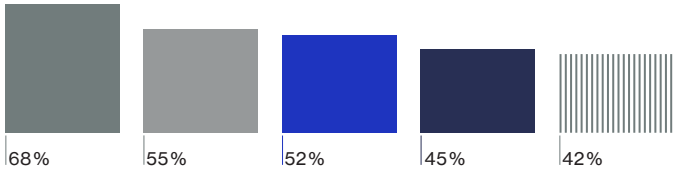
Italien



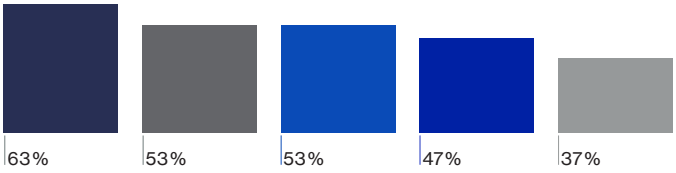
Spanien



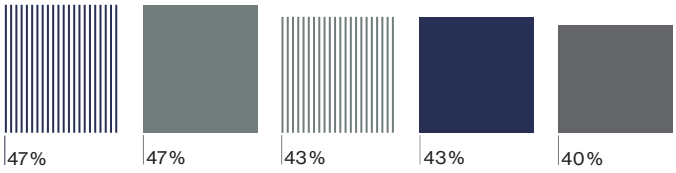
Niederlande



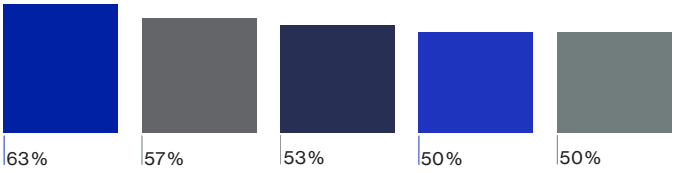
Norwegen



Schweden



Dänemark



Basis: Befragte insgesamt (346): Vereinigtes Königreich (100) Frankreich (31) Deutschland (34) Italien (30) Spanien (30) Niederlande (31) Norwegen (30) Dänemark (30)

2.4 Ein trügerisches Gefühl der Cybersicherheit

Obwohl 92% der Unternehmen in den vergangenen fünf Jahren eine Verletzung des Datenschutzes hinnehmen mussten, brachten nur 42% der Befragten Besorgnis darüber zum Ausdruck, zukünftig erneut Opfer einer Datenschutzverletzung zu werden.

92%

haben bereits Datenschutzverletzungen erlitten

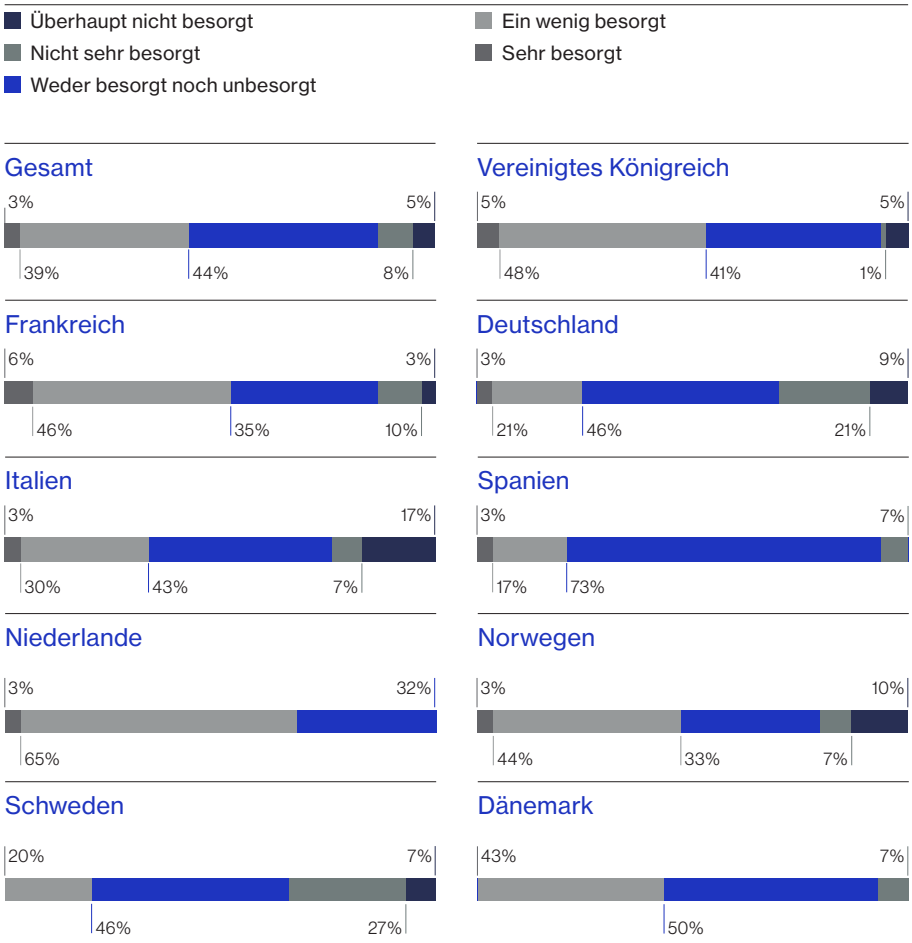
42%

befürchten, dass sie in Zukunft eine Datenschutzverletzung erleiden könnten

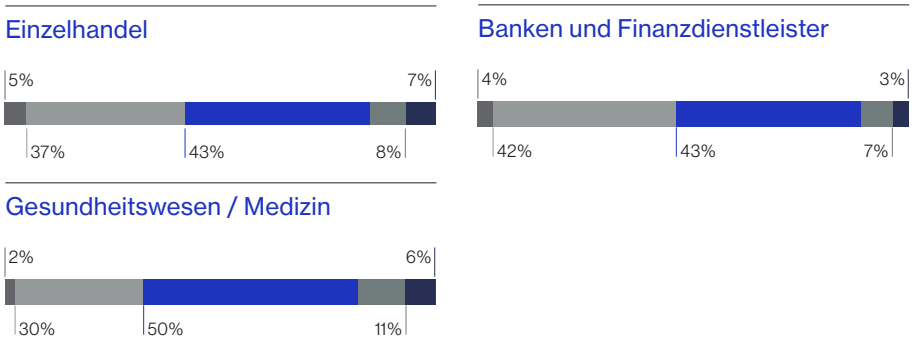
Die Ergebnisse für die einzelnen Wirtschaftssektoren waren leicht uneinheitlich. Am meisten Sorgen über Datenschutzverletzungen machten sich Finanzdienstleister (46%), was angesichts der Menge an vertraulichen Kundendaten in ihrer Obhut nachvollziehbar ist. Unternehmen des Gesundheitssektors zeigten sich weniger besorgt (32%) – eine Überraschung, weil Gesundheitsdaten wertvoller und als solche in Hackerkreisen zunehmend begehrt sind.

Diese Ergebnisse legen nahe, dass die Unternehmen entweder großes Vertrauen in ihre Cybersicherheitsmaßnahmen haben oder sich hinsichtlich ihrer Verwundbarkeit durch Cyberangriffe in trügerischer Sicherheit wiegen. Wie dem auch sei: Die für Cyberangriffe genutzte Technologie entwickelt sich ständig weiter und macht einen 100%igen Selbstschutz der Unternehmen praktisch unmöglich. Unternehmen, die Cybersicherheit jetzt nicht ausreichend ernst nehmen, werden Cyberangriffen in Zukunft relativ schutzlos ausgeliefert sein.

Wie sehr befürchten Sie, dass Ihr Unternehmen Opfer einer Datenschutzverletzung wird? Bitte geben Sie einen Wert auf einer Skala von 1 bis 5 an, wobei 1 für „überhaupt nicht besorgt“ und 5 für „sehr besorgt“ steht.



Basis: Befragte insgesamt (346): Vereinigtes Königreich (100) Frankreich (31) Deutschland (34) Italien (30) Spanien (30) Niederlande (31) Norwegen (30) Dänemark (30)



Basis: Befragte insgesamt (346): Einzelhandel (109) Banken und Finanzdienstleister (95) Gesundheitswesen / Medizin (90)

Teil 3
Vorbereitung und Reaktion

3.1 Mangelnde Vorbereitung ...

Wie bereits in Teil 2 erwähnt, haben 92 % der Unternehmen in den vergangenen fünf Jahren bereits eine Datenschutzverletzung erlitten. Nun sollten die Teilnehmer der Umfrage angeben, wie gut sie auf einen Wiederholungsfall vorbereitet sind. Hierfür beschrieben sie den Grad der Vorbereitung für den Fall einer Datenschutzverletzung anhand von drei Kriterien:

1. Organisation von Maßnahmen zur Krisenintervention: z. B. Benachrichtigung von Kunden und Aktualisierung von IT-Systemen.
2. Begrenzung des möglichen Imageschadens: z. B. durch PR-Maßnahmen, Werbung und andere Marketingaktivitäten.
3. Regulatorische Konsequenzen: z. B. Kooperation bei Untersuchungen oder den Umgang mit regulatorischen Änderungen.

93 %

der Unternehmen wären „gut vorbereitet“ oder „sehr gut vorbereitet“ auf die Organisation von Kriseninterventionsmaßnahmen

89 %

sagten dasselbe in Bezug auf die Begrenzung eines möglichen Imageschadens

87 %

über den Umgang mit regulatorischen Konsequenzen

Bei den meisten Unternehmen gibt es offenbar Abläufe und Handlungsanweisungen für Cybervorfälle, was nicht heißt, dass sie lückenlos gewappnet sind. Viele Unternehmen konzentrieren sich auf die Erstellung eines Reaktionsplans, der regelt, was im Fall einer Datenschutzverletzung zu tun ist. Daneben gibt es – vor und nach einem Datenschutzvorfall – eine ganze Reihe von Maßnahmen, die es im Hinblick auf eine optimale Vorbereitung umzusetzen gilt.

Bevor Unternehmen sich hinsichtlich ihrer Abwehrbereitschaft in Sicherheit wiegen dürfen, müssen sie eine rigorose Überprüfung und externe Validierung ihrer Systeme gewährleisten. Und auch danach gilt es, wachsam zu bleiben und die Pläne an neu auftretende Bedrohungen anzupassen.

3.2 Wer übernimmt Verantwortung?

Datensicherheit fiel einst zu hundert Prozent in den Zuständigkeitsbereich der IT-Abteilung. Inzwischen ist Datensicherheit derart wichtig, dass sie ganz oben auf der Prioritätenliste der Chefetagen steht.

Dieser Wandel ist bemerkenswert schnell vonstattengegangen. Letztes Jahr [2015] zählten einer Marsh-Umfrage zufolge nur 17% der europäischen Unternehmen Cyberrisiken zu den fünf dringlichsten ihrer Unternehmensrisiken. Bei 25% tauchten Cybervorfälle überhaupt nicht in der Liste der Risikoszenarien auf. Fast zwei Drittel der Unternehmen (65%) sagten, in erster Linie sei die IT-Abteilung verantwortlich für die Cyberrisiken des Unternehmens. Nur 11% sahen die Verantwortung bei der Unternehmensführung.

Die neun Monate später durchgeführte Lloyd's-Umfrage kam zu dem Ergebnis, dass sich das Management in europäischen Unternehmen inzwischen sehr viel unmittelbarer mit der Gefährdung durch Cyberrisiken auseinandersetzt.

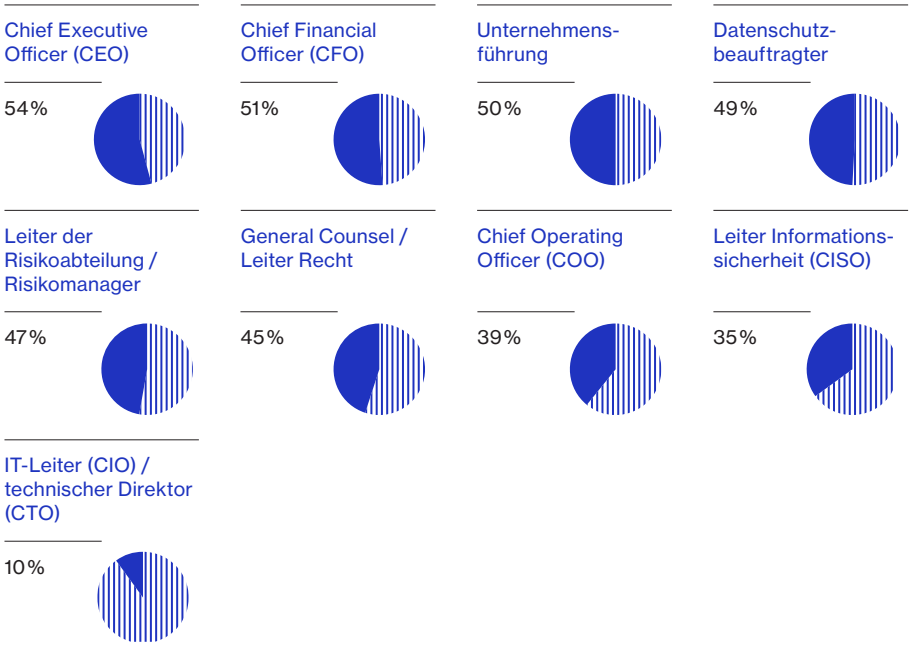
Die Befragten sollten angeben, wer in ihrem Unternehmen die Entscheidungen zum Datenschutz und zur Planung für den Ernstfall von Datenschutzverstößen trifft. Die Mehrheit der Befragten (54%) nannte in diesem Zusammenhang den Geschäftsführer (CEO). Führungskräfte, für die der Cyberraum zum Arbeitsalltag gehört, erschienen viel weiter unten auf der Liste: Nur 35% gaben an, der Funktionsbereich Informationssicherheit (CISO) sei hierfür zuständig, und lediglich 10% nannten den IT-Manager (CIO) oder den technischen Direktor (CTO). In 96% der Fälle wurde ein Angehöriger der Unternehmensführung als Entscheidungsträger genannt.

Die Annahme liegt nahe, dass die jüngste Serie medienbeherrschender Datenschutzverletzungen und deren Folgen – Einbruch von Aktienkursen, Kosten, Gerichtsverfahren – die CEOs zur Entwicklung rigoroser Cybersicherheitsstrategien veranlasst hat. Die Aktionäre erwarten, dass die Geschäftsführungen Cybersicherheit zur Chefsache machen und alles in ihrer Macht Stehende unternehmen, um die Risiken zu minimieren, die letzten Endes die finanzielle Leistung des Unternehmens gefährden.

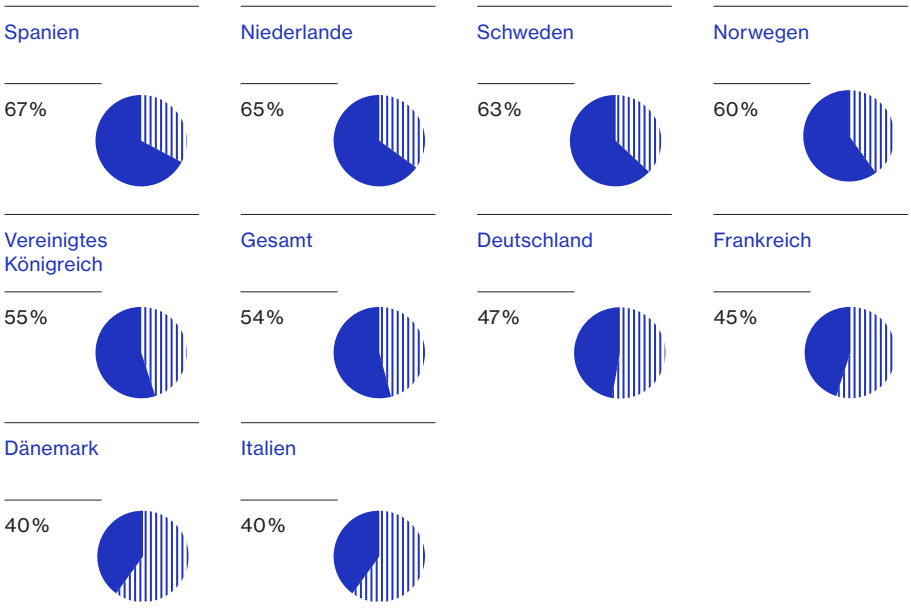
Das Thema nicht auf die leichte Schulter zu nehmen, liegt auch im Eigeninteresse der CEOs, denn im Ernstfall droht ihnen der Jobverlust. So mussten sowohl der CEO des US-Einzelhändlers Target als auch der Chef des österreichischen Flugzeugkomponentenherstellers FACC infolge einer Cyberattacke ihren Hut nehmen.

Es ist erfreulich, dass, wie die vorliegende Studie zeigt, sich immer mehr CEOs mit Cyberrisiken auseinandersetzen. Die bevorstehenden Änderungen der EU-Bestimmungen werden das Thema für alle Unternehmen in Europa in den Vordergrund rücken.

Wer trifft in Ihrem Unternehmen Entscheidungen zum Datenschutz und zur Planung für den Fall von Datenschutzverletzungen?



Chief Executive Officer (CEO)



Basis: Befragte insgesamt (346)

Teil 4
Die Datenschutz-Grundverordnung verstehen

4.1 Eine neue Ära der Cyberegulierung

Die Einführung der Datenschutz-Grundverordnung der Europäischen Union im Jahr 2018 wird die Cyberregulierung in Europa revolutionieren. Sie hat darüber hinaus weitreichende Konsequenzen für Unternehmen in aller Welt, derer sich die Betroffenen in vielen Fällen nicht bewusst sind.

Die Datenschutz-Grundverordnung schreibt Datenschutzrechte des Verbrauchers fest, z. B. ein „Recht auf Vergessenwerden“ und das Recht auf Widerspruch gegen die Erstellung persönlicher Profile (Profiling)“, welche die Unternehmen respektieren müssen.

Wichtig: Die Datenschutz-Grundverordnung betrifft nicht nur Unternehmen mit Sitz in einem der EU-Mitgliedsstaaten. Jedes Unternehmen, das EU-Bürgern Waren und Dienstleistungen anbietet oder deren Verhalten beobachtet, muss die Bestimmungen der Verordnung einhalten. Daraus folgt, dass beispielsweise auch viele Unternehmen aus den USA oder Asien in den Geltungsbereich der Datenschutz-Grundverordnung fallen.

Die neue Verordnung darf also auf keinen Fall ignoriert werden. Die Umfrage ermittelte, welche Vorkehrungen die Unternehmen im Hinblick auf die Einführung der Datenschutz-Grundverordnung in weniger als zwei Jahren treffen.

Was ist die Datenschutz-Grundverordnung?

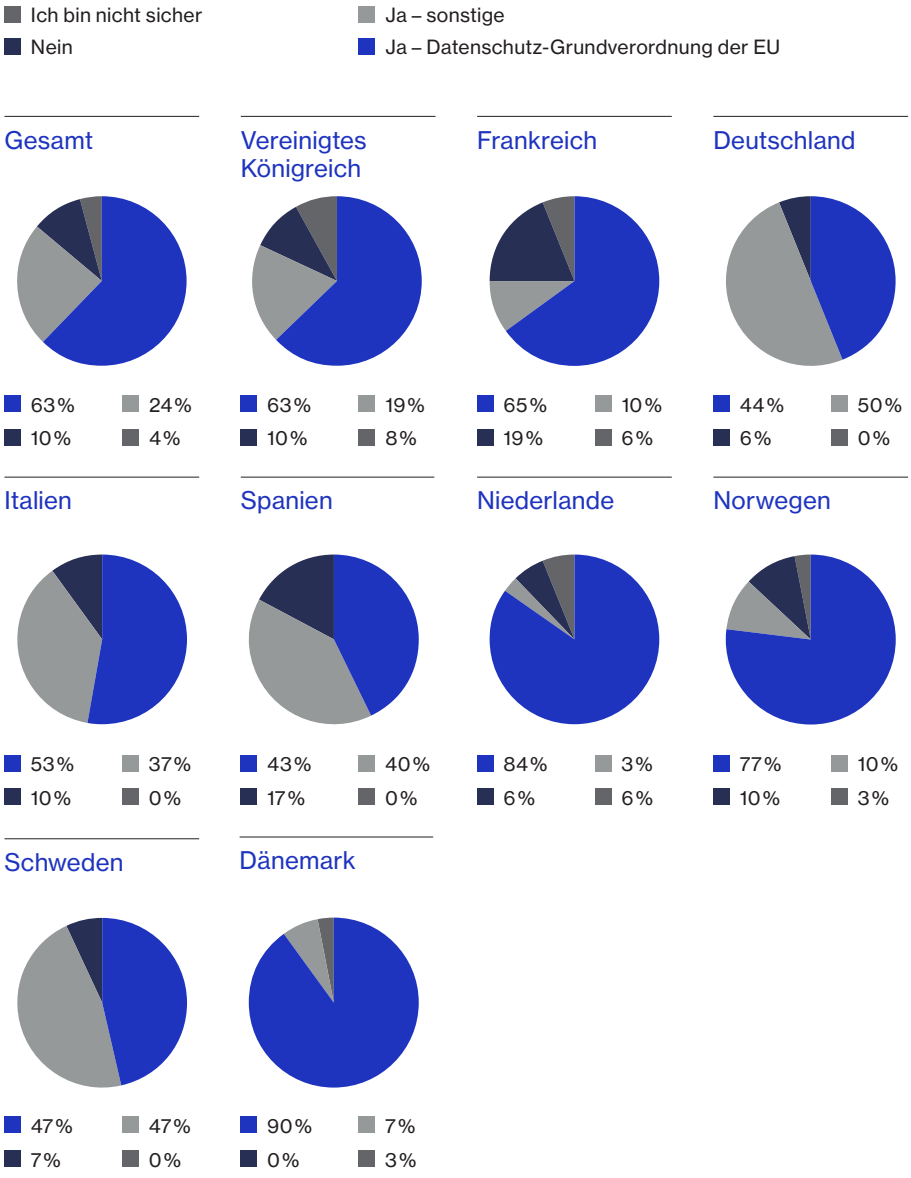
- Die Datenschutz-Grundverordnung ist ein EU-Gesetz zur Vereinheitlichung der Vorschriften zum Schutz von personenbezogenen Daten in Europa und soll die EU-Gesetzgebung zum Umgang mit den technischen Möglichkeiten des Big-Data-Zeitalters befähigen.
- Insbesondere verlangt sie, dass Datenschutzverletzungen innerhalb von 72 Stunden der zuständigen Behörde gemeldet und die betroffenen Bürger umgehend informiert werden.
- Sie sieht im Fall von Datenschutzverstößen Bußgelder von bis zu 4 % des weltweiten Jahresumsatzes bzw. 20 Millionen Euro vor, je nachdem, welcher Betrag höher ist. Auch Einzelpersonen können von Unternehmen Schadenersatz für finanzielle Verluste oder immaterielle Schäden fordern.
- Die Datenschutz-Grundverordnung tritt am 25. Mai 2018 in allen Mitgliedsstaaten der EU in Kraft, betrifft aber jedes Unternehmen, das Geschäfte mit Bürgern der EU betreibt, unabhängig vom Sitz des Unternehmens.

4.2 Kenntnis und Verständnis

Angesichts der Tragweite der Datenschutz-Grundverordnung und nachdem die jetzt unmittelbar bevorstehende Umsetzung bereits 2012 bekanntgegeben wurde, könnte man erwarten, dass die Unternehmen ausgereifte Pläne in den Schubladen haben. Die Umfrage zeigte hingegen ein uneinheitliches Bild.

Sie kam zu dem Ergebnis, dass die Mehrheit der Unternehmen von der Datenschutz-Grundverordnung weiß. Auf die Frage, ob ihnen neue Vorschriften oder Änderungen an Vorschriften mit Konsequenzen für die Datenschutzlandschaft bekannt seien, nannten 63% die Datenschutz-Grundverordnung. Weitere 24% verwiesen auf andere Vorschriften, einschließlich Änderungen an Datenschutzregelungen auf nationaler Ebene.

Wissen Sie etwas von neuen oder geänderten Vorschriften in Zusammenhang mit dem Thema Datenschutz?



Basis: Befragte insgesamt (346): Vereinigtes Königreich (100) Frankreich (31) Deutschland (34) Italien (30) Spanien (30) Niederlande (31) Norwegen (30) Dänemark (30)

4.2 Kenntnis und Verständnis

Auf die konkrete Frage nach der Datenschutz-Grundverordnung gaben 97% der Unternehmen an, sie hätten davon gehört. Das darf jedoch nicht darüber hinweg täuschen, dass Detailkenntnisse eher die Ausnahme sind. Lediglich 7% der Befragten gaben an, „sehr viel“ über die Datenschutz-Grundverordnung zu wissen, während mehr als die Hälfte (57%) zugaben, nur „wenig“ oder „gar nichts“ darüber zu wissen. Wenn man bedenkt, welche Tragweite die Datenschutz-Grundverordnung für Unternehmen hat, offenbart sich hierin ein überraschender Mangel an Information.

97%

der Befragten haben von der Datenschutz-Grundverordnung gehört

57%

räumten ein, dass die „wenig“ oder „gar nichts“ über die Datenschutz-Grundverordnung wussten

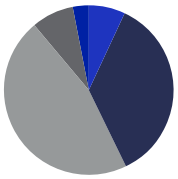
Die Datenschutz-Grundverordnung sieht zum Beispiel erhebliche finanzielle Sanktionen für Unternehmen vor, die die Verordnung nicht einhalten (bis zu 4% des weltweiten Umsatzes). Sie setzt darüber hinaus höhere Maßstäbe für die Transparenz der Verwendung von Kundendaten, die Sicherheit der Systeme zum Schutz personenbezogener Daten und die Fristen, innerhalb derer die Kunden über eine Datenschutzverletzung informiert werden müssen. Keine dieser Anforderungen ist ohne Weiteres zu erfüllen – sie alle verlangen Zeit, Investitionen und Arbeitsaufwand.

Das Umfrageergebnis legt nahe, dass Unternehmen mehr tun müssen, um die Bedeutung der Datenschutz-Grundverordnung für ihr Unternehmen und die entsprechende Verantwortung zu erfassen.

Was wissen Sie über die Datenschutz-Grundverordnung?

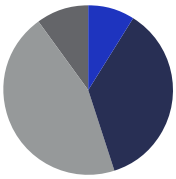
- Ich weiß sehr viel über die Datenschutz-Grundverordnung
- Ich habe von der Datenschutz-Grundverordnung gehört, kenne aber nicht viele Einzelheiten
- Ich habe noch nicht von der Datenschutz-Grundverordnung gehört und weiß nichts darüber
- Ich habe ausreichende Kenntnisse über die Datenschutz-Grundverordnung
- Ich habe von der Datenschutz-Grundverordnung gehört, kenne aber keine Einzelheiten

Gesamt



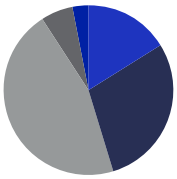
7% 36% 46% 8% 3%

Vereinigtes Königreich



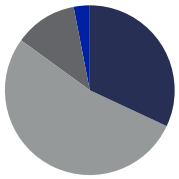
9% 36% 45% 10% 0%

Frankreich



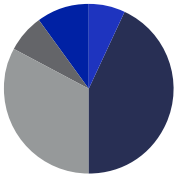
16% 29% 45% 6% 3%

Deutschland



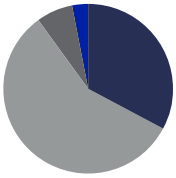
0% 32% 53% 12% 3%

Italien



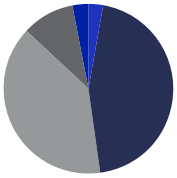
7% 43% 33% 7% 10%

Spanien



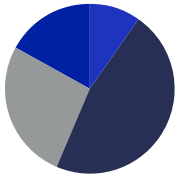
0% 33% 57% 7% 3%

Niederlande



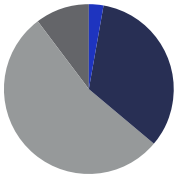
3% 45% 39% 10% 3%

Norwegen



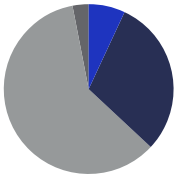
10% 47% 27% 0% 17%

Schweden



3% 33% 53% 10% 0%

Dänemark



7% 30% 60% 3% 0%

Basis: Befragte insgesamt (346): Vereinigtes Königreich (100) Frankreich (31) Deutschland (34) Italien (30) Spanien (30) Niederlande (31) Norwegen (30) Dänemark (30)

4.3 Erkennen der Konsequenzen für Unternehmen

Obwohl die Mehrheit der Führungskräfte einräumte, nur wenig über die Datenschutz-Grundverordnung zu wissen, sagten 66%, sie seien sich ihrer Konsequenzen im Fall einer Datenschutzverletzung in ihrem Unternehmen bewusst.

Auf intensivere Nachfrage ergaben sich Kernthemen: regulatorische und finanzielle Folgen. An erster Stelle standen behördliche Untersuchungen, die von 64% der Unternehmensvertreter als wahrscheinlichste Konsequenz genannt wurden. An zweiter Stelle standen Strafzahlungen oder Bußgelder (58%), gefolgt von Auswirkungen auf den Gewinn oder Aktienkurs (57%). Nur 13% äußerten Befürchtungen, Kunden zu verlieren.

64%
Behördliche Untersuchungen

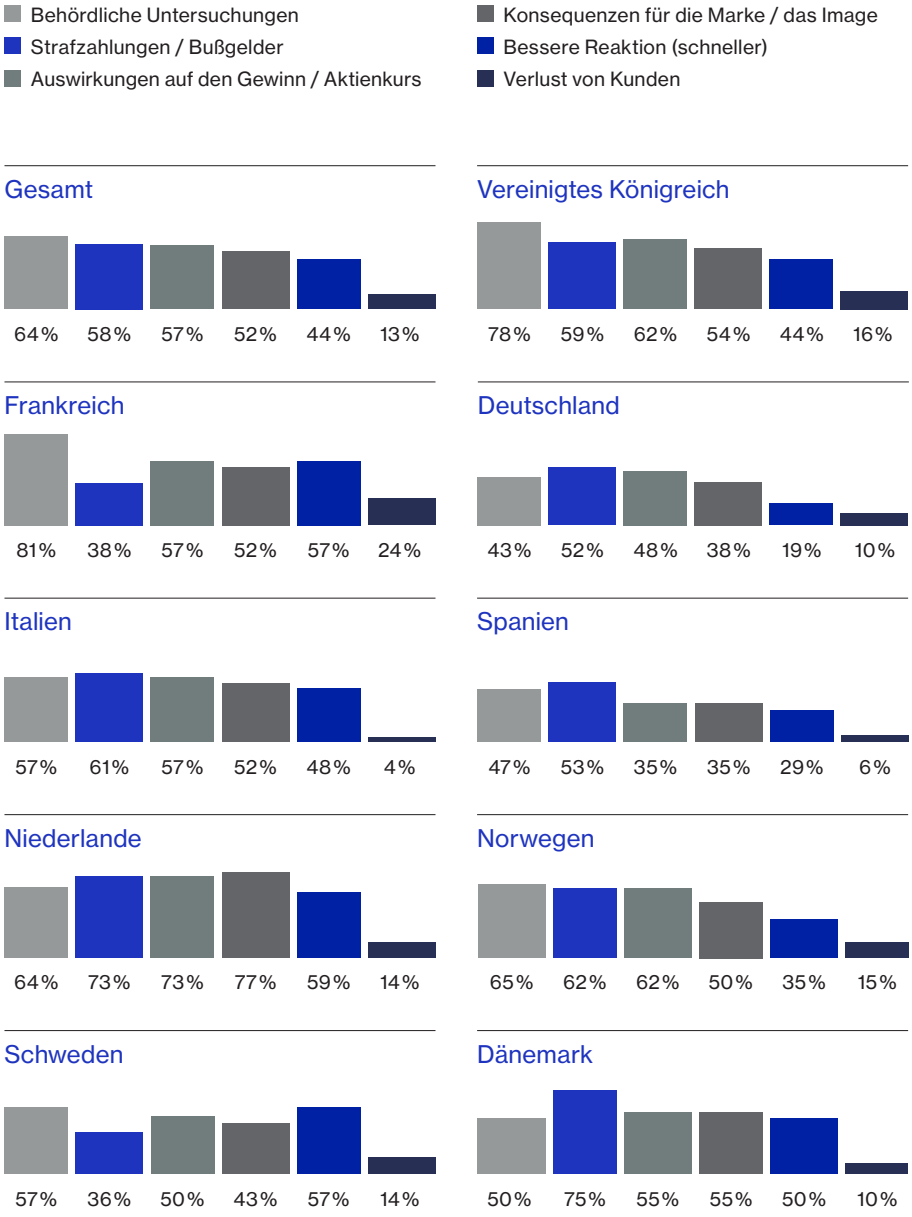
58%
Strafzahlungen oder Bußgelder

57%
Auswirkungen auf den Gewinn oder Aktienkurs

13%
Verlust von Kunden

Die Umfrage ergibt, dass große europäische Unternehmen sich insbesondere Sorgen über die möglichen finanziellen Konsequenzen der Datenschutz-Grundverordnung im Fall einer Datenschutzverletzung machen. Die Cyberattacke auf TalkTalk hat das Unternehmen beispielsweise rund 60 Mio. £ gekostet und am Tag des Bekanntwerdens zu einem Einbruch des Aktienkurses um 10% geführt. Nach den Vorschriften der Datenschutz-Grundverordnung werden die finanziellen Auswirkungen von Datenschutzverstößen voraussichtlich noch größer ausfallen.

Welche Konsequenzen wird die Datenschutz-Grundverordnung, vom Standpunkt der derzeitigen Datenschutzprozesse in Ihrem Unternehmen aus gesehen, voraussichtlich für Ihr Unternehmen haben?



Basis: Befragte insgesamt (227): Vereinigtes Königreich (63) Frankreich (21) Deutschland (21) Italien (23) Spanien (17) Niederlande (22) Norwegen (26) Dänemark (20)

Teil 5
Fazit

5.1 Fazit

Cybervorfälle sind das komplexeste, aktuellste und gefährlichste Risiko, dem Unternehmen heutzutage ausgesetzt sind: Es geht lediglich um die Frage, „wann“ und nicht „ob“ ein Unternehmen Opfer einer Datenschutzverletzung oder Cyberattacke wird.

Mit Cybervorfällen geht ein ganzes Spektrum möglicher Folgen einher: Betriebsunterbrechung, finanzielle Sanktionen, behördliche Untersuchungen und Imageschäden – allesamt eine ernsthafte Gefahr für Einnahmen, Aktienkurse oder gar die Lebensfähigkeit von Unternehmen. Vor diesem Hintergrund sind Maßnahmen zum Schutz ihrer Unternehmen keine triviale Aufgabe für Wirtschaftslenker.

Das Ergebnis der Umfrage zeigt, dass viele Unternehmen sich selbstbewusst zeigen, was die Vorbereitung auf die Datenschutz-Grundverordnung angeht, das Verständnis der möglichen Tragweite aber zu wünschen übrig lässt. Zudem legen Datenschutzverstöße neueren Datums nahe, dass die Unternehmen nicht so gut auf Cyberattacken vorbereitet sind, wie sie glauben.

Noch haben die Unternehmen 18 Monate Zeit, bis die neue Verordnung in Kraft tritt, und können ihre Abläufe und Systeme für die Einhaltung der Datenschutz-Grundverordnung optimieren. Bis dahin kommt es darauf an, dass Unternehmen ihre Cyberrisikostrategie überprüfen und ihre Gefährdungslage analysieren. Die Bedrohung aus dem Cyberraum wird nicht verschwinden und höchstens noch an Komplexität gewinnen. 100%iger Schutz vor Cyberangriffen ist praktisch unmöglich.

Nachstehend drei Empfehlungen für Wirtschaftsführer zum Schutz ihrer Unternehmen:

1 Identifizieren Sie die konkreten Risiken, denen Ihr Unternehmen ausgesetzt ist.

Ermitteln Sie die wahrscheinlichsten Möglichkeiten für eine Datenschutzverletzung in Ihrem Unternehmen. Erarbeiten Sie konkrete Pläne zur Risikominderung. Für welche unwahrscheinlichen Szenarien haben Sie keine Vorkehrungen getroffen? Sie müssen Ihre Maßnahmenpläne regelmäßig testen und aktualisieren. Am besten lassen Sie sie durch externe Berater überprüfen. Lassen Sie sich beim Durchspielen von Szenarien und Simulationen unterstützen. Etablieren Sie Maßnahmen vor und nach einem Datenschutzvorfall, nicht nur für die Benachrichtigung der betroffenen Kunden.

2 Klären Sie in Ihrem Unternehmen über Cyberrisiken und die entsprechenden Vorschriften auf.

Am Anfang vieler Cybervorfälle steht menschliches Versagen, von der versehentlichen Offenlegung bis zum Hereinfallen auf eine Phishingattacke. Das entsprechende Problembewusstsein ist eine Frage der Unternehmenskultur und muss von der Führungsspitze gefördert werden. Sorgen Sie beispielsweise dafür, dass alle Mitarbeiter geschult sind und wissen, was die Datenschutz-Grundverordnung von ihnen verlangt.

3 Bleiben Sie auf dem Laufenden.

Die Fortschritte in der Digitaltechnik gehen weiter, und dasselbe gilt für die damit einhergehenden Cyberbedrohungen. Bauen Sie eine Kultur des „kontinuierlichen Lernens“ und des Informationsaustauschs über Cyberrisiken auf. Seien Sie sich bewusst, dass Sie Cyberrisiken niemals zu 100 % ausschließen können, was Maßnahmen zur Schadensbegrenzung, z. B. eine Cyberversicherung, umso wichtiger macht.

5.2 Was Cyberversicherung leisten kann

1 Laut der vorliegenden Umfrage verfügen 73 % der Unternehmensführer nur über begrenztes Wissen über Cyberversicherung und 50 % wissen gar nicht, dass die Risiken von Datenschutzverletzungen versicherbar sind.

2 Die Cyberversicherung erbringt nach einem Cyberangriff nicht nur finanzielle Leistung, sondern bietet auch Expertenberatung zur Steigerung der Sicherheit und konkrete Unterstützung im Krisenfall.

3 Es gibt durchaus Unterschiede zwischen den Cyberpolicen. Die meisten werden jedoch die Kosten für den juristischen und forensischen Aufwand zur Ermittlung der Ursache und Verantwortung für den Datenschutzverstoß abdecken sowie die Kosten für die Benachrichtigung von Kunden und Betriebsunterbrechungskosten.

4 Von der Zusammenarbeit mit kompetenten Spezialversicherern profitiert die Sicherheitsstrategie des Unternehmens. Der Versicherer kann dem Unternehmen helfen, Risiken und Schwachstellen zu erkennen, und somit das Risiko einer Datenschutzverletzung von vornherein senken.

5 All dies dient der Absicherung der Bilanz des Einzelunternehmens und der branchenweiten Erhöhung der Standards für Cybersicherheit und Risikominderung.

Länderinformationen sind erhältlich für: Dänemark, Deutschland, Frankreich, Italien, die Niederlande, Norwegen, Schweden, Spanien und das Vereinigte Königreich.

Weitere Informationen und Kontaktdaten der Lloyd's Cyber Broker finden Sie unter www.lloyds.com/cyber