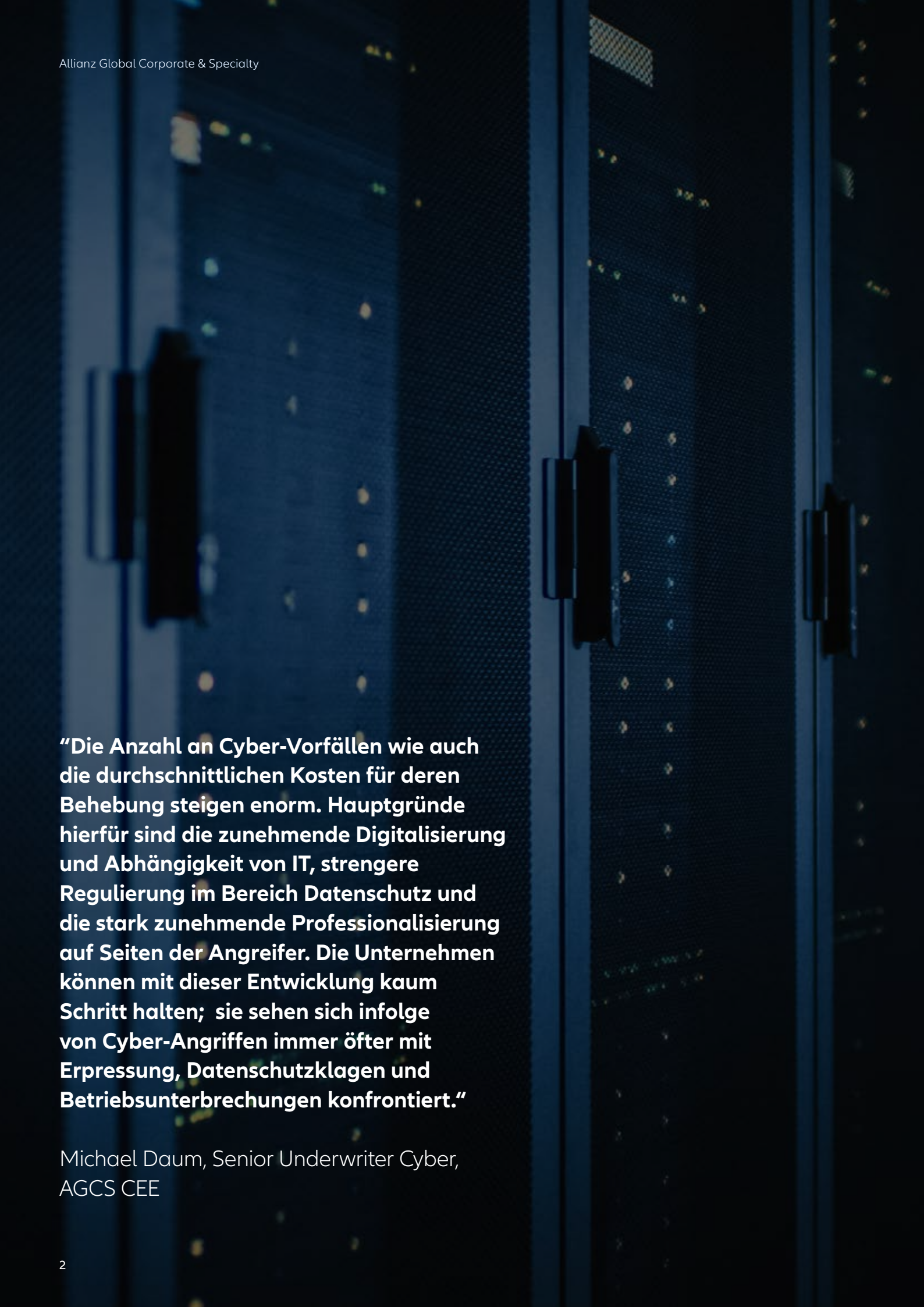
CYBER RISIKO TRENDS, DIE MAN IM AUGE BEHALTEN SOLLTE

BLICK AUF CORONA UND DARÜBER HINAUS

agcs.allianz.com

Allianz



“Die Anzahl an Cyber-Vorfällen wie auch die durchschnittlichen Kosten für deren Behebung steigen enorm. Hauptgründe hierfür sind die zunehmende Digitalisierung und Abhängigkeit von IT, strengere Regulierung im Bereich Datenschutz und die stark zunehmende Professionalisierung auf Seiten der Angreifer. Die Unternehmen können mit dieser Entwicklung kaum Schritt halten; sie sehen sich infolge von Cyber-Angriffen immer öfter mit Erpressung, Datenschutzklagen und Betriebsunterbrechungen konfrontiert.“

Michael Daum, Senior Underwriter Cyber, AGCS CEE

Cyber-Risiken nehmen weiter zu. Ein signifikanter Anstieg bei der Zahl der Vorfälle durch Ransomwareangriffe trägt dazu bei, dass sich die Schadenhäufigkeit bei Unternehmen erhöht. Insgesamt werden Cyber-Angriffe ausgereifter und gezielter, angesichts des Bestrebens von Kriminellen, durch Forderungen von mehreren Millionen Euro höhere Beträge zu erbeuten.

Im Jahre 2020 waren Cyber-Vorfälle die Nummer eins (39 % der Antworten) bei den wichtigsten Geschäftsrisiken im **Allianz Risk Barometer**. Vergleicht man dies mit 2013, als sie mit nur 6 % der Antworten auf Platz 15 rangierten, wird klar, wie schnell das Bewusstsein für Cyber-Gefahren zugenommen hat, was auch darauf zurückzuführen ist, dass Unternehmen mehr und mehr auf ihre Daten- und IT-Systeme angewiesen sind.

ALLIANZ RISK BAROMETER
RISIKO IM FOKUS: **CYBER VORFÄLLE**

GLOBALE ENTWICKLUNG DER RANGLISTE (POSITION, % DER ANTWORTEN)

- 2020: 1 (39%)
- 2019: 2 (37%)
- 2018: 2 (40%)
- 2017: 3 (30%)
- 2016: 3 (28%)
- 2015: 5 (17%)

TOPRISIKO IN DEN FOLGENDEN LÄNDERN

- Österreich
- Belgien
- Frankreich
- Indien
- Malaysia
- Südafrika
- Südkorea
- Spanien
- Schweden
- Schweiz
- Großbritannien
- USA

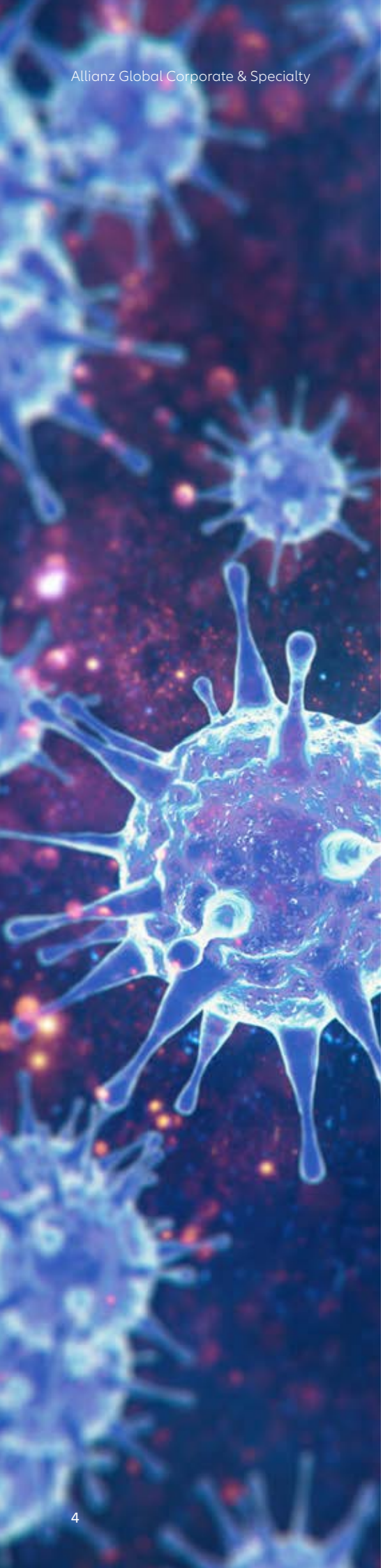
TOPRISIKO IN DEN FOLGENDEN SEKTOREN

- Luftfahrt
- Finanzdienstleistungen
- Staat und Verwaltung
- Professionelle Dienstleistungen
- Technologie
- Telekommunikation

ALLIANZ RISK BAROMETER 2020

Das Allianz Risk Barometer ist der Jahresbericht der AGCS, in dem die wichtigsten Unternehmensrisiken für die nächsten 12 Monate und darüber hinaus identifiziert werden, und zwar auf Grundlage der Erkenntnisse von über 2.700 Risiko-Management-Experten aus 102 Ländern. Im Jahr 2020 waren Cyber-Vorfälle erstmalig das wichtigste Geschäftsrisiko weltweit.

Das Bewusstsein für die Cyber-Gefahr ist in den letzten Jahren drastisch gestiegen, da sich Unternehmen zunehmend auf Daten und IT-Systeme verlassen, aber auch aufgrund aufsehenerregender Vorfälle. Vor 7 Jahren rangierten sie noch auf Platz 15. Nachzulesen unter www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer



CORONAVIRUS

Mit der verstärkten Nutzung des Homeoffice aufgrund der Corona-Pandemie **steigt die Zahl der Cyber-Angriffe**. Hacker, Scammer und Spammer suchen nach Schwachstellen, um an wertvolle Daten zu gelangen.

Das Coronavirus ändert die tägliche Arbeitsweise und Interaktion zwischen den Menschen. Viele Unternehmen sahen sich infolge der Pandemie gezwungen, ihre Remotekapazität auszubauen - und das geschah in den meisten Fällen sehr kurzfristig. Um möglichst vielen Mitarbeitern einfachen Zugriff auf Betriebssoftware und -systeme zu bieten, müssen in manchen Fällen u. U. die IT-Sicherheitsstandards gesenkt oder ausgesetzt werden, was die Unternehmen potenziellen Gefahren für die Cyber-Sicherheit aussetzt.

Laxere Sicherheitsvorkehrungen können dazu führen, dass es **Internetkriminellen und Hackern einfacher gemacht wird, in zuvor effektiv geschützte Unternehmenssysteme einzudringen**, was zu Datenschutzverstößen, Übergriffen von Cyber-Erpressern und Ausfällen von IT-Systemen führen kann. Schätzungsweise 50 bis 90 % der Datenschutzverstöße werden von Mitarbeitern ausgelöst oder begünstigt, sei es, dass es sich dabei um einen einfachen Fehler handelt oder dass man Phishing oder Social Engineering zum Opfer fällt.

Unglücklicherweise verschärft die Tatsache, dass pandemiebedingt wesentlich mehr Leute von Zuhause aus arbeiten und dabei auf das Firmennetz mittels einer VPN-Verbindung zugreifen, diese Risiken noch weiter und eröffnet Cyber-Kriminellen ausgezeichnete Gelegenheiten; das veranschaulichen aktuelle Ereignisse nur zu gut.

Phishing-Versuche im Rahmen des Coronavirus mit schädlichen Links oder Anhängen, die per E-Mail- oder WhatsApp-Nachricht verschickt werden, sind seit Januar 2020 im Umlauf; seither steigt ihre Zahl. Die Europäische Kommission erklärt, dass die Cyber-Kriminalität in der EU seit Beginn des Ausbruchs zunehme, während die Weltgesundheitsorganisation (WHO) kürzlich vor verdächtigen E-Mails warnte, über die die Covid-19 Notlage ausgenutzt würde [1], um die Öffentlichkeit um ihr Geld und sensible Daten zu bringen. In einigen Ländern ist **die Zahl der versuchten Cyber-Angriffe** zwischen Mitte Februar und Mitte März um das **Fünffache** gestiegen.
Im April entdeckte und blockierte Google in einer einzigen Woche über 18 Mio. Schadsoftware- und Phishing-E-Mails und 240 Mio. Spam-Nachrichten täglich in Zusammenhang mit der Pandemie [2]. Insgesamt blockiert der Tech-Riese pro Tag über 100 Mio. Phishing-Emails.

[1] World Health Organization, Beware of criminals pretending to be WHO, 2020
[2] Google Cloud, Protecting Businesses Against Cyber Threats During Covid-19 And Beyond

In einem kürzlich erschienenen Risk Bulletin der AGCS wurden verschiedene Maßnahmen empfohlen, die IT-Sicherheit im Homeoffice zu erhöhen, darunter:

- Software-Aktualisierung
- Aktivierung von Virenschutz und Firewalls
- extreme Vorsicht beim Austausch personenbezogener Daten - Online-Betrüger verbessern ihre Erfolgsrate, indem sie ihre Opfer persönlich ansprechen
- Sicherstellen, dass Webbrowser auf dem neuesten Stand sind
- sichere Aufbewahrung von Passwörtern und deren regelmäßige Änderung. Die allgemeine Regel für die Wahl des Passwortes: je länger, desto besser
- Schutz vertraulicher E-Mails durch Verschlüsselung
- Herunterladen von Daten ausschließlich von vertrauenswürdigen Quellen
- Durchführung regelmäßiger Backups
- Abschaltung von sprachaktivierten intelligenten Geräten und Abdecken von nicht benutzten Webcams
- Klare Unterscheidung zwischen Geräten und Informationen für betriebliche und private Nutzung, kein Transfer von Aufgaben zwischen den beiden Bereichen. Dies verhindert unbeabsichtigte Datenlecks
- Identifizierung aller Teilnehmer in Online-Sitzungen
- Abmelden von Geräten, die nicht mehr in Betrieb sind, und deren sichere Aufbewahrung
- Sicherheitspraktiken für Ausdrucke und Umgang mit vertraulichen Dokumenten
- Vorsicht bei verdächtigen E-Mails oder Anhängen, insbesondere von unbekanntem Absender

Die vollständige Übersicht über die IT-Sicherheitsmaßnahmen laden Sie bitte das Bulletin herunter:
https://bit.ly/ARC-Coronavirus

ÜBER DAS CORONAVIRUS HINAUS

CYBER TRENDS DIE MAN IM AUGE BEHALTEN SOLLTE

WAS SIND DIE HAUPTURSACHEN VON CYBER-VORFÄLLEN?

77%

1. Datenschutz- oder Sicherheitsverstoß
(z. B. Zugriff auf/Löschung von personenbezogenen/ vertraulichen Daten)

62%

2. Spionage, Hackerangriffe, Erpressungssoftware, Denial-of-Service-Angriffe

42%

3. Irrtum oder Fehler von Mitarbeitern

Quelle: Allianz Global Corporate & Specialty - Zahlen stehen für den Prozentsatz der Antworten aller Teilnehmer (1.071), die am Allianz Risk Barometer 2020 teilgenommen haben. Die Summe der Prozentwerte ergibt nicht 100 %, weil bis zu drei Risiken ausgewählt werden konnten.

TREND

Größere und kostenaufwendigere Datenschutzverstöße

Da die Unternehmen immer größere Volumina personenbezogener Daten erheben und verwenden, werden Datenschutzverstöße immer umfangreicher und kostenaufwendiger. Insbesondere sogenannte Mega-Datenverstöße (mit mehr als 1 Mio. Datensätzen) kommen häufiger vor und sind kostspielig. Im Juli 2019 legte Capital One offen, dass der Finanzdienstleister einer der bisher größten Datenschutzverletzungen im Bankensektor zum Opfer gefallen war; ca. 100 Mio. Kunden waren davon betroffen. Allerdings ist dieser Fall von Datenschutzverletzung keineswegs der größte in den letzten Jahren.

Vergleichbare Fälle bei der Hotelgruppe Marriott im Jahre 2018 und dem Finanzdienstleister Equifax im Jahre 2017 erstreckten sich auf personenbezogene Daten von 300 Mio. bzw. 140 Mio. Kunden. Beide Firmen sahen sich etlichen Gerichtsverfahren und behördlichen Maßnahmen an diversen Gerichtsständen ausgesetzt. Die britische Datenschutz-behörde beabsichtigt, Mariott mit einer Geldstrafe von 100 Mio. GBP (aktuell 110,75 Mio. EUR) für diese Verletzung zu belegen, bislang eine der am schnellsten verhängten und höchsten Geldauflagen im Rahmen der neuen Datenschutzgesetze der EU.

Im selben Monat, also im Juli 2019, wurde British Airways vorläufig mit der Zahlung einer Geldstrafe von 183 Mio. GBP (202,67 Mio. EUR) für einen Datenschutzverstoß, dem 500.000 Kunden im Jahre 2018 zum Opfer gefallen waren, belegt.

Die Datenschutz-Grundverordnung (DSGVO), die in Europa 2018 in Kraft trat, wird aller Voraussicht auch im Jahre 2020 und danach zu weiteren hohen Geldbußen führen. Der europäische Datenschutzausschuss (EDSA) veröffentlichte einen vorläufigen Bericht [1], aus dem hervorgeht, dass im Rahmen der DSGVO von den 206.436 in den ersten neun Monaten seit ihrer Umsetzung gemeldeten Fällen aus 31 Ländern nur ca. 50 % von den nationalen Datenschutzbehörden gelöst werden konnten. Die Regulierungsbehörden haben sich also durch diesen Rückstand gekämpft, sodass mehr Strafen mit höheren Bußgeldern registriert wurden.

Ein Megadaten-Verstoß kostet laut Ponemon Institute mittlerweile im Schnitt 42 Mio. USD [2], was einem Anstieg von nahezu 8 % gegenüber 2018 entspricht. Bei Verstößen mit über 50 Mio. Datensätzen werden die Kosten auf 388 Mio. USD geschätzt; sie liegen somit 11 % über dem Niveau von 2018.

[1] European Data Protection Board, First Overview On The Implementation Of The GDPR And The Roles And Means Of The National Supervisory Authorities.
[2] IBM Security, Ponemon, Cost Of A Data Breach Report, 2019.

TREND

Erpressungssoftware führt vermehrt zu Verlusten

Der Europäischen Strafverfolgungsbehörde zufolge ist Erpressungssoftware die bedeutendste Art der Bedrohung durch Cyber-Kriminalität. Die jetzt schon hohe Zahl der Vorfälle löst immer höhere Schäden aus, wobei vermehrt große Unternehmen ins Visier genommen und mit raffinierten Angriffen und extremen Erpressungsforderungen traktiert werden. Fünf Jahre zuvor hätte sich eine typische Forderung im Zusammenhang mit Erpressungssoftware auf einige zehntausend Euro belaufen. Heutzutage sind es bisweilen sogar Millionen.

Die Konsequenzen eines Angriffs können lähmend sein, insbesondere für Unternehmen, die sich zur Bereitstellung ihrer Produkte und Dienstleistungen auf Daten verlassen. Und Erpressungsforderungen sind nur ein Aspekt von vielen. Betriebsunterbrechungen lösen die schwerwiegendsten Schäden durch Erpressungssoftware-Angriffe aus. In manchen Fällen verschleiert die Erpressungssoftware nur das eigentliche Ziel, etwa den Diebstahl personenbezogener Daten. Industrie- und Gewerbebetriebe stehen immer öfter im Visier, doch besonders schwer wiegen die Folgen von Angriffen bei Anwaltskanzleien oder Beratungs- und Architekturbüros, die von IT-Systemen und Daten auf Gedeih und Verderb abhängen.

Störfälle, wie sie das Schadsoftware-Programm Ryuk verursacht hat, erwiesen sich in der jüngsten Vergangenheit als Hauptverantwortliche für Cyber-schäden. Ryuk ist nach einer fiktionalen Manga-Figur benannt und wurde erstmalig im August 2018 publik. Etliche Angriffe auf größere Unternehmen, Krankenhäuser und Lokalbehörden weltweit gehen auf Ryuk zurück.

TREND

Angriffe durch sog. Business E-Mail Compromise führen zu Betrug in Milliardenhöhe

Angriffe durch Business E-Mail Compromise (BEC) – oder Spoofing – nehmen an Häufigkeit zu. Laut dem US-amerikanischen FBI haben BEC-Vorfälle seit 2016 zu weltweiten Schäden von mindestens 26 Mrd. USD geführt.

Die Angriffe laufen in der Regel über Social Engineering Methoden und Phishing-E-Mails, die Mitarbeiter oder die oberen Führungskräfte in betrügerischer Absicht dazu verleiten, Anmeldedaten preiszugeben oder Betrugsgeschäfte abzuschließen.

TREND

Prozesswahrscheinlichkeit steigt

Zahlreiche schwerwiegende Datenschutzverstöße ziehen heutzutage aufsichtsrechtliche Maßnahmen nach sich, doch sie können auch rechtliche Schritte seitens der betroffenen Verbraucher, Geschäftspartner und Investoren auslösen. Wenn dies der Fall ist, können Rechtskosten die Ausgaben erheblich in die Höhe treiben.

Rechtsstreitigkeiten wegen Datenschutzverstößen sind ein sich entwickelndes Phänomen in den USA. Etliche schwerwiegende Verstöße haben zu Sammelklagen von Verbrauchern oder Investoren geführt – im Juli 2019 erzielte Equifax einen Vergleich in Höhe von 700 Mio. USD für seinen Megadaten-Verstoß im Jahre 2017. US-Gerichte haben sich mit Fragen der Klagebefugnis herumgeschlagen – unabhängig davon, ob die Antragsteller das Klagerecht haben – doch der Trend scheint zugunsten der Kläger zu gehen. Gesetzliche und aufsichtsrechtliche Änderungen könnten auch die Durchsetzbarkeit von Entschädigungen für Datenschutzverstöße erhöhen. Der California Consumer Privacy Act sieht z. B. einen Mechanismus vor, über den Verbraucher Unternehmen verklagen können, und legt – erstmalig in den USA – gesetzlichen Schadenersatz im Falle von Datenschutzverstößen fest.

Außerhalb der USA haben einige Länder die Sammelklagerechte ausgeweitet. So macht es in Europa die DSGVO Opfern einer Verletzung des Datenschutzes oder der Privatsphäre einfacher, ihre Rechte gerichtlich geltend zu machen. Darüber hinaus bemühen sich die Anwaltskanzleien der Antragsteller und Prozesskostenfinanzierer aktiv darum, bei Datenschutzverstößen auch in Europa und andernorts Sammelklagen anzustrengen. Eine solche wurde kürzlich gegen British Airways aufgrund ihres Datenschutzverstoßes im Jahre 2018 von den britischen Gerichten zugelassen. Verbrauchergruppen sind zudem bestrebt, die DSGVO zu testen und die Auslegung des neuen Gesetzes durch einige Unternehmen zu hinterfragen.

TREND

Fusionen und Übernahmen können Cyber-Probleme verursachen

Cyber-Gefahren sind nach einigen weitreichenden Datenschutzverstößen zu einem heißen Thema bei Fusionen und Übernahmen (Mergers & Acquisitions, M&A) geworden. So ließ sich der Datenschutzverstoß bei Mariott im Jahre 2018 auf ein Eindringen bei Starwood 2014, einer Hotelgruppe, die das Unternehmen 2016 übernommen hatte, zurückverfolgen. Selbst die am besten geschützten Unternehmen sind gefährdet, wenn sie eine Firma mit geringer Cyber-Sicherheit oder bestehenden Schwachstellen übernehmen. Das erwerbende Unternehmen könnte für Schäden aus Vorfällen haftbar gemacht werden, die vor dem Zeitpunkt der Fusion datieren.

Letztendlich müssen Unternehmen der Berücksichtigung potenzieller Cyber-Schwachstellen und -Risiken bei Fusionen und Übernahmen eine höhere Priorität einräumen, da viele von ihnen in diesem Bereich ihrer Sorgfaltspflicht nicht hinreichend nachkommen. Gleichzeitig lassen sich etliche Firmen nach Abschluss eines Deals zu viel Zeit, um Schwachstellen bei den übernommenen Systemen zu beheben.

TREND

Politische Faktoren spielen im Cyber-Bereich eine Rolle

Dass mittlerweile auch Nationalstaaten in Cyber-Angriffe involviert sind, stellt ein zunehmendes Risiko für Unternehmen dar. Nicht nur ihr geistiges Eigentum sehen sie bedroht, sie stehen auch im Visier bestimmter Gruppen, die absichtlich Störungen oder Sachschäden herbeiführen. So haben wachsende Spannungen im Nahen Osten dazu geführt, dass internationale Transporte das Ziel von Spoofing-Angriffen im Persischen Golf wurden, während Gas- und Ölförderanlagen Cyber-Angriffen und Erpressungssoftware-Kampagnen zum Opfer fielen. Ausgeklügelte Angriffstechniken und Schadsoftware können zudem auch zu Cyber-Kriminellen durchsickern. Die Beteiligung von Nationalstaaten bedeutet auch eine bessere Bezahlung für Hacker. Selbst wenn Unternehmen nicht das unmittelbare Ziel sind, können Cyber-Angriffe mit staatlicher Unterstützung Kollateralschäden verursachen. Der NotPetya-Schadsoftware-Angriff im Jahre 2017 richtete sich in erster Linie gegen die Ukraine, verbreitete sich jedoch rasch weltweit.

WAS IST DER BESTE ANSATZ ZUR BEHERRSCHUNG VON CYBER-RISIKEN UND ZUR VERBESSERUNG DER WIDERSTANDSKRAFT GEGENÜBER CYBER-ANGRIFFEN?

1 55%

Cyber-Risiken sind Teil unseres allgemeinen Unternehmensrisikos und gelten als eines der wichtigsten wirtschaftlichen Risiken.

2 52%

Überwachung und Messung von Systemsicherheit und -verfügbarkeit durch kontinuierliche Bewertungen von Risiko und Schwachstellen, Gegenmaßnahmen und Informationsaustausch in Sachen Cyber-Bedrohungen.

3 45%

Regelmäßige Mitarbeiterschulungen zu Informationssicherheit, Sensibilisierungs- und Anti-Phishing-Kampagnen.

Quelle: Allianz Global Corporate & Specialty. Die Zahlen zeigen den Prozentsatz der Antworten aller Teilnehme (1.071), die am Allianz Risk Barometer 2020 teilgenommen haben. Die Summe der Prozentwerte ergibt nicht 100 %, weil bis zu drei Risiken ausgewählt werden konnten.

RISIKOMINDERUNG

Vorbereitung und Schulung sind die effizientesten Formen der Risikobegrenzung und können die Wahrscheinlichkeit oder Folgen eines Cyber-Vorfalls maßgeblich reduzieren. Zahlreiche Vorfälle gehen auf menschliches Versagen zurück, das durch entsprechende Schulungen verringert werden kann, insbesondere in Bereichen wie Phishing und Business e-Mail Compromise, die zu den verbreitetsten Formen von Cyber-Attacken zählen.

Schulungen könnten auch zudem beitragen, Angriffe durch Erpressungssoftware abzumildern, obschon bereits die Aufrechterhaltung sicherer Backups potentielle Schäden begrenzen kann. Die Widerstandsfähigkeit des Unternehmens und die Planung für eine Geschäftsfortführung sind ebenfalls essentiell für die Verringerung der Auswirkungen eines Cyber-Vorfalls. Notfallpläne für Cyber-Krisen müssen freilich getestet, eingeübt und regelmäßig überprüft werden.

“Der Erwerb von Cyber-Deckung sollte einer der abschließenden Maßnahmen innerhalb eines betrieblichen Risikomanagements zur Stärkung der Widerstandsfähigkeit gegenüber Cyber-Angriffen sein. Versicherung trägt entscheidend dazu bei, dass Unternehmen sich nach einem Angriff erholen, sollten sich alle anderen Maßnahmen als unzureichend erweisen. Sie sollte das strategische Risikomanagement jedoch nicht ersetzen.
Die Investition in die Sensibilisierung der Mitarbeiter aber auch die Aktualisierung und kontinuierliche Überwachung von Systemen sollten definitiv ganz oben auf der Prioritätenliste eines jeden Unternehmens stehen.”

Jens Krickhahn, Practice Leader Cyber & TECH/MEDIA
AGCS CEE

WENDEN SIE SICH AN UNS

Das Cyber-Team der Allianz Global Corporate & Specialty (AGCS) steuert Fachwissen und Erkenntnisse bei, die uns dabei helfen, innovative und flexible Lösungen für unsere Kunden bereitzustellen.

KONTAKTE IN ÖSTERREICH:

SEVERIN GETTINGER
severin.gettinger@allianz.at

GABOR SAS
gabor.sas@allianz.at

Über Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) ist ein weltweit führender Anbieter von Unternehmensversicherungen und gehört zur Allianz Gruppe. Wir bieten Risikoberatung, Schaden- und Unfallversicherung und alternativen Risikotransfer für ein breites Spektrum von Firmen-, Industrie- und Spezialrisiken in zwölf Geschäftssparten.

Unsere Kunden sind so vielfältig wie die Geschäftswelt, angefangen von den Fortune Global 500-Unternehmen bis hin zu Kleinbetrieben und Privatpersonen. Darunter sind führende Konsumgütermarken, Technologieunternehmen und die globale Luft- und Schifffahrtsindustrie ebenso wie Weinkellereien, Satellitenbetreiber oder Hollywood-Filmproduktionen. Sie alle zählen auf intelligente Lösungen für ihre größten und komplexesten Risiken in einem dynamischen, multinationalen Geschäftsumfeld. Sie verlassen sich darauf, dass wir ihnen mit umfassendsten Schadenerfahrungen helfen können.

Weltweit ist die AGCS mit eigenen Teams in 32 Ländern sowie über das Netzwerk der Allianz Gruppe und Partner in über 200 Ländern und Gebieten tätig. Sie beschäftigt insgesamt mehr als 4.300 Mitarbeiter. Als eine der größten Schaden- und Unfallversicherungseinheiten der Allianz Gruppe verfügen wir über starke und stabile Finanzratings. Im Jahr 2019 erwirtschaftete die AGCS weltweit Bruttoprämien in Höhe von insgesamt 9,1 Milliarden Euro.

www.agcs.allianz.com/about-us/about-agcs.html

Folgen Sie der Allianz Global Corporate & Specialty auf

Twitter **@AGCS_Insurance**

LinkedIn

Weitere Informationen zur AGCS finden Sie unter
www.agcs.allianz.com

Allianz Global Corporate & Specialty SE
Königinstr. 28, 80802 München,
Handelsregister: München HRB 208312

Photos: Adobe Stock

September 2020