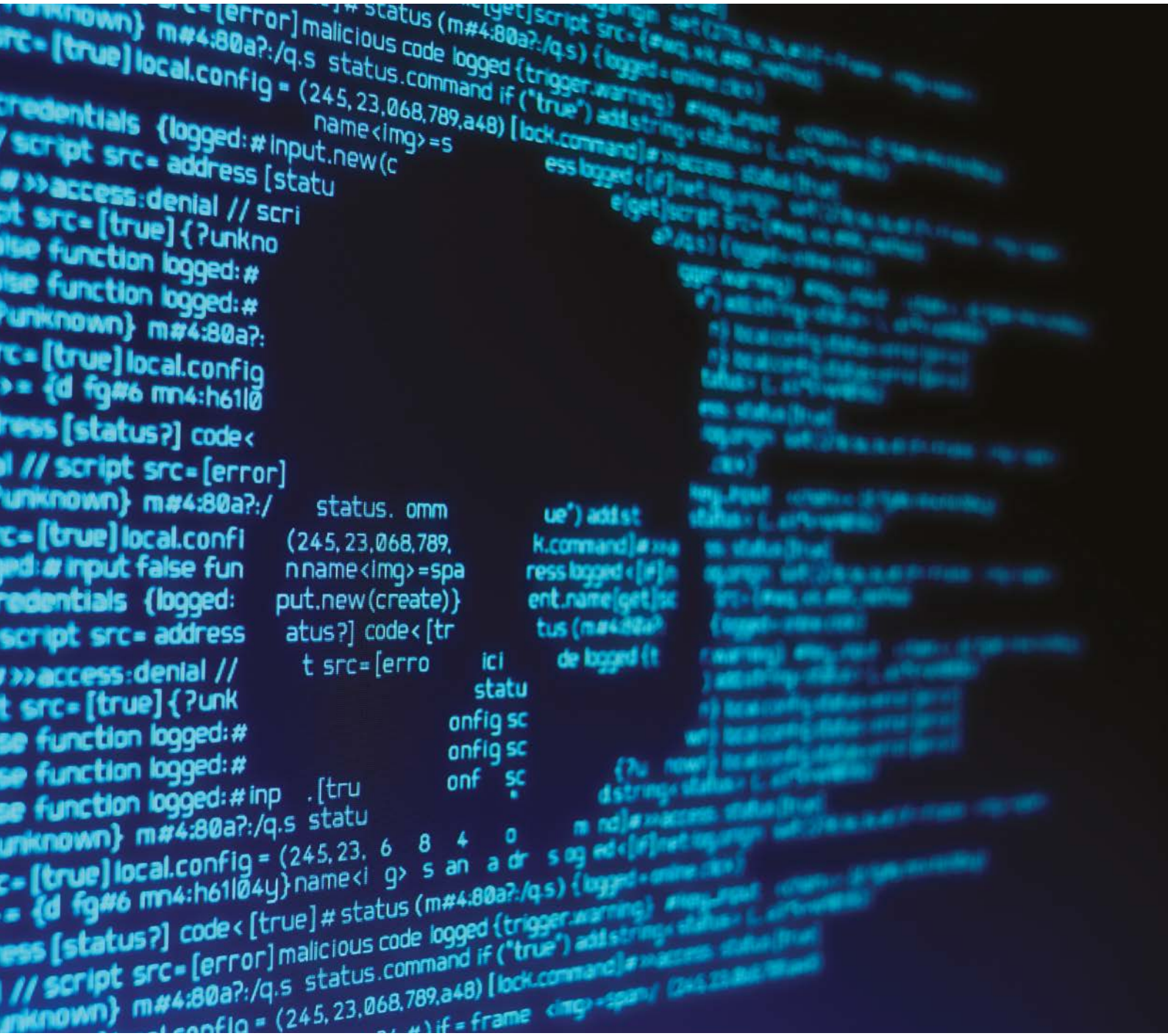
Claims Intelligence Series



Der große Hintergrundbericht: Ransomware bringt den Geschäftsbetrieb zum Erliegen

Die Ergebnisse des diesjährigen AIG Cyber-Schadenreports zeigen bei Versicherungen aus dem Jahr 2017 eine starke Zunahme an Cyber-Schäden auf. Gleichzeitig kam es in den vergangenen Monaten verstärkt zu komplexen Angriffserien durch systemische Schadsoftware und Ransomware, darunter WannaCry und NotPetya. Deutlich wurde auch: Für viele europäische Unternehmen waren Betriebs- und Netzwerkunterbrechungen ein wichtiges Thema, bei dem jedoch die Mehrheit der entstandenen Schäden nicht durch Versicherungen gedeckt war.

Wie bereits Anfang letzten Jahres von den Cyber-Experten der AIG prognostiziert, war das Jahr 2017 geprägt von Ransomware-Angriffen und Betriebsunterbrechungen durch Cyber-Vorfälle. Die Schaden-Statistiken zeigen, dass über ein Viertel der 2017 gemeldeten Cyber-Schäden (26 %) auf Ransomware als Hauptursache zurück zu führen sind. Im Vergleich: Von 2013 bis 2016 waren es nur 16 %.

„Die Tatsache, dass sich Unbefugte die Tools der NSA für einen Angriff zunutze gemacht haben, ist in dieser Dimension neu", so Nepomuk Loesti, Head of Liabilities, Financial Lines und Client Engagement bei AIG. „Durch die Ransomware WannaCry waren hunderttausende technische Anlagen weltweit betroffen. Schlussendlich war es jedoch reiner Zufall, dass ein Forscher den "Kill Switch" - den Notschalter - gefunden hat. Wäre dies nicht der Fall gewesen, wäre der wirtschaftliche Schaden weitaus höher ausgefallen."

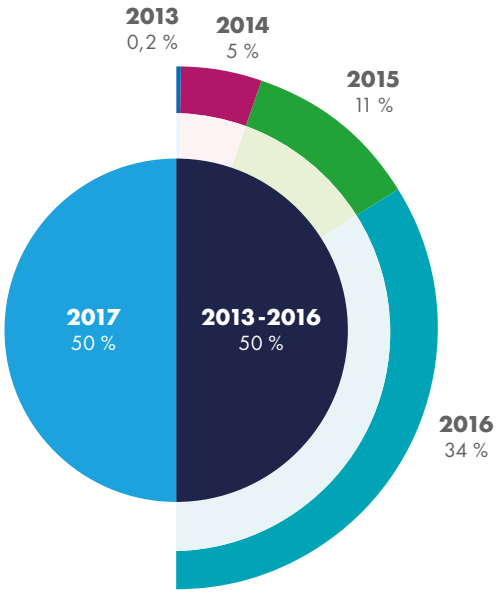
Neben Ransomware bezogen sich Cyber-Schäden vor allem auf Datenschutzverletzungen durch Hacker, sonstige Sicherheitsprobleme bzw. unberechtigte Zugriffe und Identitätsbetrug. Obwohl der Anteil der durch nachlässiges Verhalten von Mitarbeitern entstandenen Schäden in 2017 auf 7 % geringfügig zurückgegangen ist, spielt das menschliche Versagen bei der Mehrheit der Cyber-Schäden nach wie vor eine wesentliche Rolle.

Auf einen Blick

- Im Jahr 2017 gingen so viele Schadenmeldungen bei AIG ein wie in den vorangegangenen vier Jahren zusammen. Dies entspricht einem Schadenfall pro Arbeitstag.
- Dabei sind die weltweit immer häufiger auftretenden Ransomware-Angriffe die Hauptursache für Cyber-Schäden – mit Betriebsunterbrechungen als wesentlichem Effekt.
- Die Bereiche der professionellen Dienstleistungen, Finanzdienstleistungen sowie der Einzelhandel stehen dabei ganz oben auf der Liste der Cyber-Schäden. Aber auch in allen möglichen anderen Bereichen kommt es zu entsprechenden Vorfällen, was zeigt, dass mittlerweile keine Branche mehr gegen Cyber-Angriffe immun ist.

Abb. 1: **Cyber-Schadenmeldungen bei AIG EMEA (2017) – nach Ursache**

Abb. 2: **Cyber-Schadenmeldungen bei AIG EMEA (2013 - 2017) – Volumen**

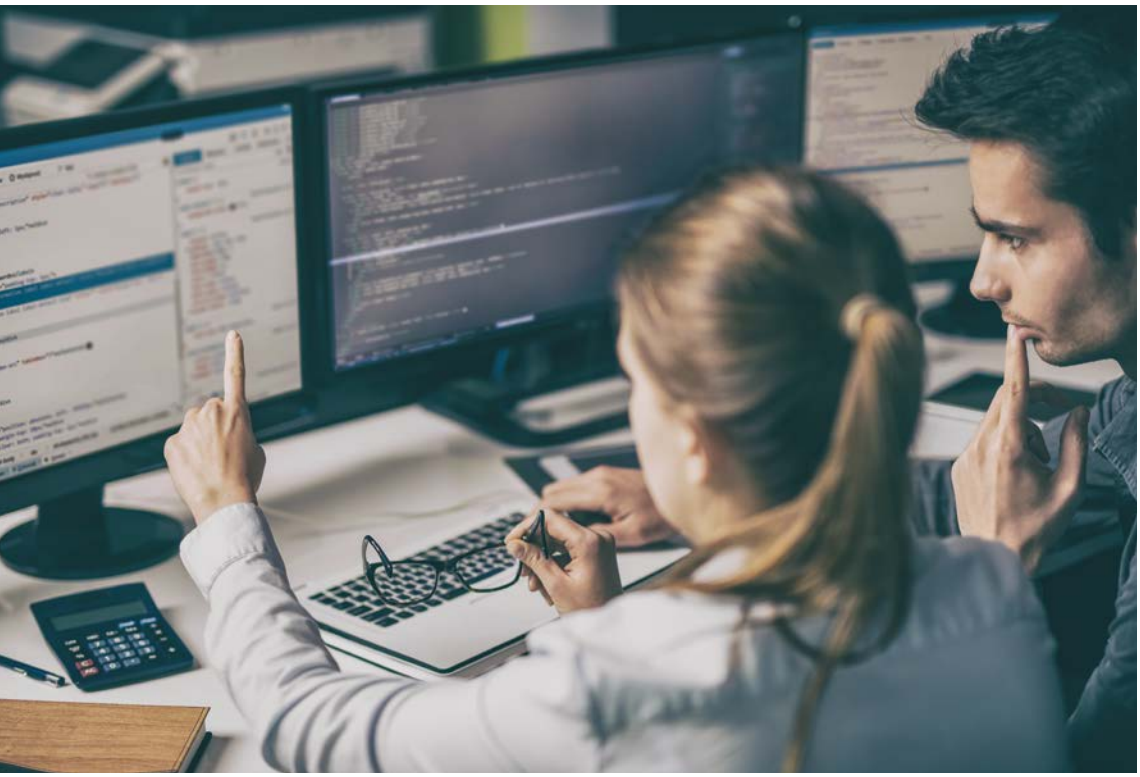


Auch die Häufigkeit der Schadenmeldungen ist im vergangenen Jahr erneut gestiegen. In 2017 bearbeiteten die Cyber-Experten bei AIG durchschnittlich einen Schadenfall pro Arbeitstag. Diese Zunahme deutet gleichsam auf eine steigende Tendenz zur Ausweitung von Cyber-Schäden hin.

Da immer mehr Unternehmen standardmäßig eine Cyber-Versicherung abschließen, machen sich die Versicherungsnehmer zunehmend mit dem Produkt vertraut. Sie verstehen besser, welche Schäden durch die Versicherung gedeckt sind und welche Vorfälle sie ihrem Versicherungsunternehmen melden könnten und sollten.

Infolge einer Welle von systemischen Ransomware- und Denial-of-Service-Angriffen (DDoS) werden inzwischen deutlich häufiger Cyber-Versicherungen abgeschlossen. Es kann jedoch passieren, dass diese Entwicklung möglicherweise wiederum zu einer höheren Schadenhäufigkeit führen wird: „Das Thema Cyber ist in den vergangenen Monaten immer stärker in den Fokus der Unternehmen geraten. Deutlich wird dies besonders dadurch, dass aktuell vermehrt solche Unternehmen Interesse an einer Absicherung bekunden, die in der Regel eher keine Cyber-Versicherung abschließen. Es ist also zu erwarten, dass es in den nächsten Jahren zu einer Zunahme an Schadenfällen kommen wird“, so Loesti.

„Die Cyber-Versicherung etabliert sich immer mehr als Standard im deutschsprachigen Markt.“ Nepomuk Loesti



Eine Bedrohung für alle Branchen

Der Schadenreport zeigt weiterhin, dass mittlerweile keine Branche mehr gegen Cyber-Angriffe immun ist. Im vergangenen Jahr meldeten allein acht Branchen Cyber-Schäden, die zuvor noch nie in der AIG Cyber-Schadenstatistik aufgetaucht sind. Hierbei handelt es sich um einen anhaltenden Trend; jedes Jahr gehen mehr und mehr Schadenmeldungen aus immer diverseren Branchen ein. Zu diesen zählen inzwischen nicht mehr nur diejenigen, die traditionell mit Cyber-Risiken in Verbindung gebracht werden, sondern beispielsweise auch der Energiesektor und das Transportwesen.

Während ein Großteil der Schadenmeldungen weiterhin auf Finanzdienstleistungen entfällt, sank der prozentuale Anteil dieser Branche im Jahr 2017 auf 18 % (23 % in den Jahren 2013 bis 2016). Aufgrund des speziellen Charakters des Banken- und Versicherungsgeschäfts sowie der Menge an Daten, die durch Finanzinstitute (FIs) nicht nur verwaltet wird, sondern auch strengen Bestimmungen (und potenziell hohen Geldstrafen) unterliegt, war diese Branche schon immer auf ein solides, umfangreiches Konzept hinsichtlich Cyber-Risiken angewiesen.

Abb. 3: **Cyber-Schadenmeldungen bei AIG EMEA (2017) – nach Branche**

*Nahrungsmittel und Getränke, Bauwesen, Immobilien, Landwirtschaft, Informationsdienstleistungen
Anmerkung: Aufgrund rundungsbedingter Abweichungen ergeben die Werte möglicherweise keine 100 %.

Die Reduktion des prozentualen Anteils der von FIs gemeldeten Schäden spiegelt möglicherweise das stetige Wachstum von Angriffen auf andere Branchen wider und zeigt die steigende Vielfalt der Cyber-Versicherungsnehmer von AIG EMEA. Loesti erläutert dazu Folgendes: „Die Finanzdienstleistungsbranche war historisch gesehen immer eine der größten Bereiche für uns als Versicherer. In den vergangenen Jahren hat sich jedoch herausgestellt, dass es hier eine Verschiebung gibt: Der Versicherungsschutz für Cyber-Risiken wird mittlerweile immer stärker auch von vielen anderen Branchen nachgefragt."

Loesti fügt hinzu: „Viele der jüngsten Ransomware-Angriffe waren völlig willkürlich. Unabhängig von bestimmten Unternehmen oder Branchen schlagen Cyber-Kriminelle vermehrt dort zu, wo die Sicherheitsbarriere am niedrigsten ist. Oder anders gesagt: Wenn die Systeme der Nutzer Sicherheitslücken aufweisen, ist die Gefahr hoch, dass sie Opfer eben solcher Pauschalangriffe werden. Aus diesem Grund blicken wir gespannt auf die Entwicklungen in 2018."

Im Bereich der professionellen Dienstleistungen zeigt sich ein erhebliches Wachstum in der Zahl der Gesamtschäden. Lag diese in den Jahren 2013 bis 2016 noch bei insgesamt 6 %, so war in 2017 ein rasanter Anstieg auf 18 % zu verzeichnen. Der prozentuale Anteil anderer Branchen, die gemeinhin eher mit Cyber-Schäden in Verbindung gebracht wurden, sank hingegen. „Professionelle Dienstleistungen wurden häufiger zum Ziel von Datendiebstahl", sagt Oliver Delvos, Senior Underwriter und Teamleiter der Cyber-Abteilung bei AIG für die DACH-Region. „Rechtsanwälte und Steuerberater mit großen Kundendatenbanken sind für Cyber-Kriminelle aufgrund der Qualität der Daten, die sie speichern, besonders attraktiv; gleiches gilt allerdings auch für Angriffe, die auf normale Finanztransaktionen abzielen."

Weiter konkretisiert er: „Die Einstellung ‚Das wird mir schon nicht passieren' oder ‚Ich habe keine Daten, die für andere von Interesse sind, warum sollte mich also jemand angreifen?' ist nach wie vor insbesondere an den Führungsspitzen weit verbreitet. Doch selbst wenn ein Unternehmen keine „interessanten" Daten speichert, kann es dennoch zum Opfer von Erpressung durch Ransomware werden. Und schlussendlich gilt für jedes Unternehmen: Wenn Dateien erst einmal verschlüsselt sind, geht nichts mehr".

„Dienstleistungsunternehmen sowie Betriebe in spezialisierten Branchen stehen immer häufiger im Visier von Cyber-Kriminellen." Oliver Delvos

Ransomware wird standardisiert

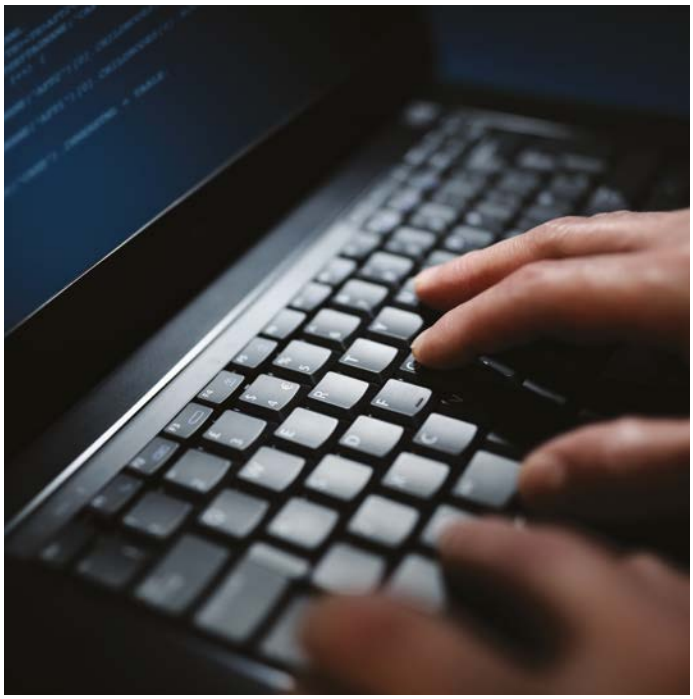
Im vergangenen Jahr waren Unternehmen in vielen europäischen Ländern von großen systemischen Ereignissen betroffen. WannaCry nutzte eine Sicherheitslücke in Windows, um Schadsoftware auf hunderttausende Geräte in über 150 Ländern zu verbreiten. Betroffen waren Unternehmen zahlreicher Branchen, einschließlich des Gesundheitswesens, Finanzdienstleistungen, Logistik, Bildung und Produktion.

In den vergangenen 24 Monaten wurden Ransomware-Angriffe immer standardisierter. Die Programmierer neuerer Versionen bieten inzwischen Vereinbarungen zur Beteiligung an den Erlösen für Teilnehmer an Partnerprogrammen. Das heißt, dass selbst für den Fall einer Lösegeldzahlung durch die Versicherten keine Garantie für eine Rückgabe der Daten existiert. Von der „Professionalität" früherer Angriffsserien, bei denen Callcenter die Opfer anriefen, um ihnen Bitcoins zur Zahlung des Lösegelds anzubieten, damit sie anschließend ihre Daten zurückerlangen konnten, ist inzwischen kaum noch etwas zu spüren.

Ransomware-as-a-Service (Ransomware als Dienstleistung) stellt jedoch für Unternehmen noch immer eine Bedrohung dar. Auch wenn Unternehmen nicht glauben, dass ihre Daten wichtig oder gefährdet sind, zeigte der Schadenverlauf für 2017, dass Ransomware-Angriffe weitgehend willkürlich erfolgen und Unternehmen aller Branchen und Größen treffen können. Experten bei AIG gehen davon aus, dass sich der Trend zur Automatisierung und Standardisierung von Ransomware weiter fortsetzen wird, sodass Unternehmen und Einzelpersonen einer immer größeren Anzahl von Angreifern ausgesetzt sein werden.

Darüber hinaus wird eine Verlagerung des Schwerpunktes in Richtung „Cryptojacking" erwartet.[1] Im Laufe des Jahres 2017 stieg der Kryptowährungsmarkt um mehr als 1.200 %.[2] Der steigende Wert elektronischer Währungen hat jedoch auch die Aufmerksamkeit von Cyber-Kriminellen geweckt, die verstärkt Netzwerke übernehmen und Schadsoftware zur Suche nach Kryptowährungen verwenden.

Es wird erwartet, dass traditionellere Formen der Erpressung zukünftig bei Datensicherheitsverletzungen eine Rolle spielen und zielgerichteter ablaufen werden. Dieser Trend macht sich zurzeit auf dem US-Markt bemerkbar und hat auch bereits zu Schäden bei europäischen Unternehmen, insbesondere bei denjenigen mit Niederlassungen in den USA, geführt. Die EU-Datenschutz-Grundverordnung (DSGVO) könnte dabei ebenfalls zu einem Werkzeug von Erpressern werden: Durch das Wissen, dass unter den neuen Gesetzen härtere Konsequenzen bei einem Bruch des Datenschutzes folgen, wird die Androhung, Daten von Unternehmen bei Nichtzahlung offen zu legen, zu einem effizienten Druckmittel.



Netzwerkunterbrechung: Ein schwerwiegender Schaden

Die Schadenstatistiken des aktuellen Reports zeigen, dass Betriebsunterbrechungen (im Rahmen der Betriebsunterbrechung durch Cyber-Vorfälle als „Netzwerkunterbrechung" bezeichnet) im Vergleich zu den Jahren 2013 bis 2016 als wichtigste Verlustursache zurück gegangen sind. Nichtsdestotrotz stellte die Unterbrechung der Geschäftstätigkeit für viele europäische Unternehmen ein ernsthaftes Problem dar. Da jedoch Schäden aufgrund von Netzwerkunterbrechung nur eine von vielen Schadenursachen waren, wurden sie nicht immer als die wichtigste Ursache genannt. Folglich sind sie in der Schadenstatistik unterrepräsentiert.

„Vielen Versicherten ist das Ausmaß eines Angriffs bei einer Erstmeldung nicht klar - sie können dieses schlichtweg nicht richtig einschätzen", erläutert Tobias Caspar, Cyber Risk Consultant bei AIG für die DACH-Region. „Meist wird davon ausgegangen, dass „nur" Schadsoftware installiert wurde oder jemand versucht, sie zu erpressen. Es bedarf in den meisten Fällen eines forensischen Teams, welches den Angriff und dessen Auswirkungen genauer betrachtet. Erst dann wird den Unternehmen häufig klar, welchen Einfluss eine Cyber-Attacke auf ihre Geschäftstätigkeiten hat. Erst dann realisieren sie, dass sie vollumfänglich nicht mehr auf ihre Daten zugreifen können oder ihre Webseite offline ist."

[1] https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#48b90c4d5ae8

[2] https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#53e14c226eed

Viele Unternehmen haben immer noch keine Cyber-Versicherung, die den Schaden einer Netzwerkunterbrechung trägt. Bei vielen finanziellen Auswirkungen, die während der Ransomware-Angriffe im letzten Jahr entstanden sind, handelte es sich beispielsweise um Bilanzverluste (siehe Kasten).

Bei der Analyse der in 2017 gemeldeten Schäden wird deutlich, dass sich das Ausmaß der durch Netzwerkunterbrechung entstandenen Verluste je nach Dauer, Unternehmensgröße und Branche stark unterscheiden kann. So beliefen sich die im vergangen Jahr von AIG Europe getragenen Schäden durch Netzwerkunterbrechung auf 3.250 US-Dollar bis zu 5,2 Millionen US-Dollar.

Laut Sebastian Hess, Cyber Risk Engineer bei AIG für die DACH-Region, leiden Versicherte, die keine umfangreiche Cyber-Versicherung abgeschlossen haben und/oder nicht über Backups ihrer Daten verfügen, am meisten unter einer Netzwerkunterbrechung infolge eines Ransomware-Angriffs: „Insbesondere kleine und mittlere Unternehmen (KMU) sollten stärker dahingehend sensibilisiert werden, dass sie leichtes Ziel sein können. Meist sind ihre Systeme nicht so robust; Backups werden nur von Zeit zu Zeit erstellt."

Weiterhin konkretisiert er: "Es ist daher wichtig für Unternehmen zu verstehen - egal ob Großkonzern oder mittelständischer Betrieb - dass Backups dabei helfen können, ein System wieder herzustellen. Nur durch eine solche Absicherung besteht in der Folge die Möglichkeit, Lösegeldforderungen leichter zu ignorieren."

Hess fügt hinzu: „In diesen Fällen werden die finanziellen Schäden größer, je länger sich die Sache hinzieht. 2017 sind wir sehr viel häufiger als in den Jahren zuvor von Versicherten gefragt worden, ob unsere forensischen Partner von KPMG sie in Bezug auf Ransomware – der Entschlüsselung von Daten und den Import früherer Backups – unterstützen können. Neben der forensischen Unterstützung haben einige von ihnen zudem begonnen, Ansprüche für Schäden aufgrund von Betriebsunterbrechungen einzureichen, weil sie nicht auf ihre Systeme und Daten zugreifen konnten oder Mitarbeiter nach Hause schicken mussten."

„Krisenpläne und das Erstellen von Backups müssen zur festen Regel werden und dürfen nicht weiterhin Ausnahme bleiben." Sebastian Hess

Geschäftsunterbrechung nach wie vor stark unterversichert

Auch 2017 waren Geschäftsunterbrechungen auf Grund verschlüsselter Daten durch Ransomware und anderer Angriffe in vielen Fällen nicht versichert. Die aus den Medien bekannten Ransomware-Angriffe waren nicht zwangsläufig auf finanziellen Gewinn aus, sondern wurden auch von staatlich geförderten Tätern initiiert, die für Störungen sorgen sollten.

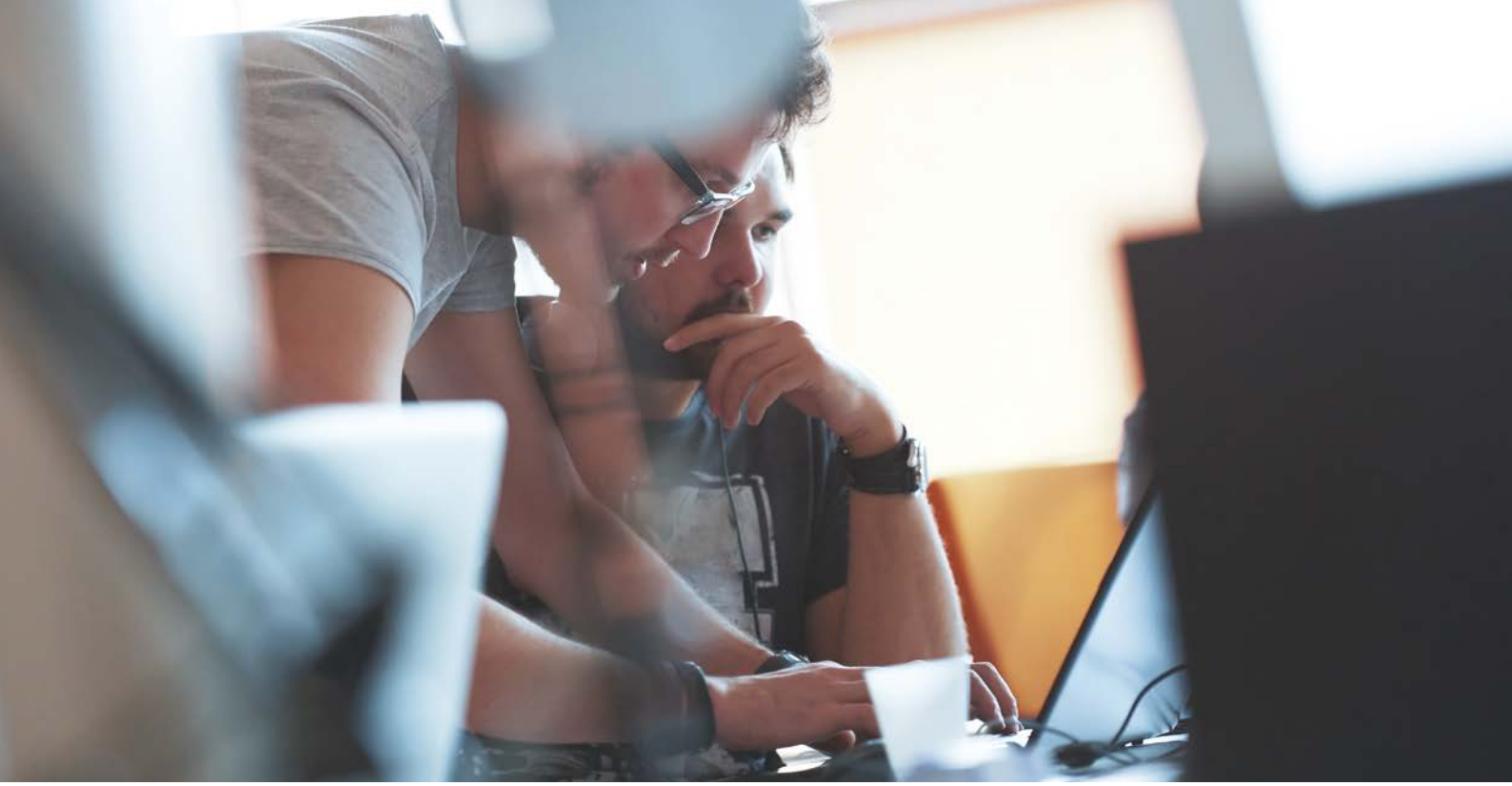
Dies ist ihnen in einem großen Ausmaß gelungen und hätte weitaus schlimmer sein können, wenn WannaCry sich unbemerkt weiterverbreitet hätte. Während sich die Lösegeldzahlungen auf einen Betrag unter 150.000 US-Dollar beliefen, liegt der wirtschaftliche Gesamtschaden durch WannaCry bei schätzungsweise 8 Milliarden US-Dollar[3], wobei eine halbe Milliarde US-Dollar[4] auf direkte Kosten und indirekte Geschäftsunterbrechungen entfallen.

Schadsoftware und Ransomware werden immer ausgefeilter, daher ist zu erwarten, dass Schäden in Zusammenhang mit Geschäftsunterbrechungen weiter steigen. Obwohl die Bedrohung einer Netzwerkunterbrechung für Unternehmen erheblich ist, fehlt aktuell das nötige Bewusstsein für dieses wichtige Thema.

„Es ist erstaunlich, dass das Thema Geschäftsunterbrechung noch relativ stiefmütterlich behandelt wird, obwohl die Unterbrechung der gesamten Wertschöpfungskette für die meisten Unternehmen einschneidende finanzielle und wirtschaftliche Folgen haben kann", so Tobias Caspar.

[3] https://uk.reuters.com/article/uk-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUKKBN1A20AH

[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-cyber-risk-outlook-2018.pdf



Die DSGVO führt die Liste der Datenschutzthemen an.

Nach dem Inkrafttreten der DSGVO am 25. Mai 2018 ist mit einem sprunghaften Anstieg der Schäden durch Datenschutzverletzungen und anderen Sicherheitsprobleme zu rechnen. Unternehmen werden Datenschutzverletzungen eher melden, was hinsichtlich Cyber-Schäden hierzulande ähnliche Auswirkungen haben wird, wie man sie in den USA beobachten konnte, nachdem dort entsprechende Gesetze in Kraft getreten sind.

„Vielen kleineren Versicherten wird zwar geraten, eine Meldung zu erstatten, aber nach den bisher geltenden Gesetzen waren sie dazu selten verpflichtet", sagt Delvos. „Nach dem Inkrafttreten der DSGVO im Mai wird dies allerdings keine Option mehr sein. Wir rechnen daher fest mit einem Anstieg der Meldungen nach diesem Termin."

Er weist darauf hin, dass es nach dem Bekanntwerden des Datenskandals von Cambridge Analytica und Facebook zu einer Verhaltensänderung in Bezug auf personenbezogene Daten gekommen ist. Dies könne sich auch auf die Art der Schäden die 2018 gemeldet werden auswirken, da Verbraucher eine Verletzung ihrer personenbezogenen Daten bei Weitem nicht mehr so einfach akzeptieren werden, wie dies in der Vergangenheit der Fall war.

"In Großbritannien ist erst vor kurzem ein Schaden durch Datenschutzverletzung an einer Universität entstanden, schildert Delvos. „Unsere Kollegen berichteten, dass die Schadenmeldung so verfasst war, als wäre die DSGVO bereits in Kraft getreten. Schlussendlich stellte sich dieser Vorfall nicht nur als kostspielig heraus, sondern führte auch zu einer Herausforderung was die Handhabung des entstandenen Reputationsrisikos betraf.

Die Benachrichtigung von 100.000 Menschen kann einen schneeballartigen Effekt haben und zu einer überaus großen Sache werden. Manche Menschen reagieren besorgt, wenn sie Benachrichtigungen über Datenschutzverletzungen erhalten, auch wenn es nur als Vorsichtsmaßnahme geschieht."

Die gemeinschaftliche Klage, die Mitarbeiter des Supermarktriesen Morrisons bei britischen Gerichten eingereicht haben, wird als wichtiger Präzedenzfall dafür gesehen, wie Gerichte Betroffene von Datenschutzverletzungen zukünftig entschädigen werden. So forderten die Mitarbeiter des Konzerns für „Ärger und Unannehmlichkeiten" durch den Diebstahl personenbezogener Daten von fast 100.000 Mitarbeitern im Jahr 2014[5] eine entsprechende Entschädigung.

Weiterhin wird erwartet, dass es durch Einführung der DSGVO künftig zu mehr Aktionärsklagen gegen Unternehmen und ihre Geschäftsführer kommen könnte. In den USA existierten über Jahre hinweg strenge Anzeigepflichten und nahezu jede Datenschutzverletzung größeren Ausmaßes wurde von mindestens einer Sammelklage begleitet.

Während in Europa noch kein vergleichbares Ausmaß an Prozessfreudigkeit und kollektiver Rechtsdurchsetzung erkennbar ist, könnte die Morrisons-Entscheidung in Zukunft den Weg für ähnliche Verfahren ebnen. „Wenn im Fall Morrisons für die emotionale Belastung durch Datenverlust eine finanzielle Entschädigung zugesprochen wird, wäre dies bemerkenswert und würde einen interessanten Präzedenzfall schaffen", sagt Loesti. „Dieser könnte ähnliche Maßnahmen gegen Unternehmen ins Rollen bringen, die die Öffentlichkeit über eine Datenschutzverletzung informieren."

[5] https://www.independent.co.uk/news/business/news/morrisons-data-leak-staff-payout-details-sensitive-data-personal-online-hack-a8086521.html

„Die meisten D&O-Policen werden Aktionärsklagen infolge von Datenschutzverletzungen nicht ausschließen, sodass solche Policen in diesen einfachen Fällen ausreichen können“, führt er weiter aus. „Durch die Einführung der DSGVO kommen Elemente wie Strafen und Bußgelder dazu. Dies führt zu einer starken Unsicherheit; besonders da davon auszugehen ist, dass diese in diesem Jahr nun erstmals auftreten können - je nachdem wie offensiv Aufsichtsbehörden mit den neuen Gesetzen umgehen werden.“

Gemäß DSGVO gibt es zwei Arten von Geldstrafen, welche gegen die Unternehmen verhängt werden können, die sich nicht ausreichend um die notwendigen Systeme und Sicherheitsmaßnahmen zum Schutz der Daten Dritter bemüht haben. Die erste beläuft sich auf bis zu 10 Millionen Euro oder 2 % des Gesamtumsatzes des Vorjahres, je nachdem welche Summe höher ist. Die zweite beläuft sich auf bis zu 20 Millionen Euro oder 4 % des Gesamtumsatzes des Vorjahres.

„Botnetze, automatisierte Angriffe und das “klassische” Social Engineering stellen auch weiterhin große Herausforderungen dar.“ Tobias Caspar

Unternehmen verfügen häufig nicht über Abwehrsysteme gegen DDoS-Angriffe

Zwei Jahre nachdem das Botnetz Mirai den DNS-Provider Dyn lahmgelegt hat, stellen DDoS-Schwachstellen immer noch eine Bedrohung dar. Die Problematik: Nach wie vor schützen Unternehmen ihre Netzwerke nicht ausreichend vor eben solchen Angriffen.

Die neueste Variante ist das Botnetz Reaper. Es besteht wie Mirai aus einer großen Anzahl von ungesicherten Heimgeräten, die das Internet der Dinge (Internet of Things, IoT) bilden, darunter Heimrouter, IP-Kameras und Babymonitore.

„Das Botnetz Reaper besteht hauptsächlich aus IoT-Geräten, die 1,6 Terabits pro Sekunde übertragen können – das ist eine riesige Datenmenge“, sagt Martin Overton, Cyber-Spezialist für EMEA bei AIG. „Botnetze von solch enormer Größe sind nach wie vor präsent; jedoch kümmern sich viele Unternehmen nicht um die notwendigen Abwehrmaßnahmen. Dabei deutet momentan nichts darauf hin, dass dieser Trend nachlassen wird.“

Mittlerweile gibt es auf dem Markt eine Reihe von Lösungen, mit deren Hilfe die Systeme während einer Attacke am Laufen gehalten werden können. Allerdings installieren viele Unternehmen nach wie vor keinen DDoS-Schutz. Kleine und mittlere Betriebe werden zudem von den Kosten abgeschreckt.

Fazit: Zeit für einen Cyber-Gesundheitscheck?

AIG geht davon aus, dass die erheblichen finanziellen Folgen einer Betriebs-/Netzwerkunterbrechung auch 2018 nochmals weiter zunehmen werden, sodass nicht nur die Nachfrage nach Versicherungslösungen steigen, sondern auch der Cyber-Versicherungsmarkt in Europa weiter wachsen wird. Aufgrund dieses steigenden Wachstums besteht gleichermaßen die Erwartung, dass sich Schadenhäufigkeit und möglicherweise auch die Schwere der Schäden erhöhen werden.

Auch in den nächsten 12 Monaten werden die Schadentrends weiterhin von einer Standardisierung der Ransomware, einem starken Anstieg von Schäden durch Datenschutzverletzungen aufgrund des Einflusses der DSGVO im späteren Verlauf des Jahres und dem fortlaufenden Einfluss staatlicher Akteure in einem immer fragileren und politisch unsicheren Umfeld geprägt sein. Traditionelle Cyber-Erpressung und Identitätsbetrug zählen somit zu den Trends, die wir im Auge behalten müssen – Angestellte stehen bei der Abwehr solcher Angriffe an vorderster Front.

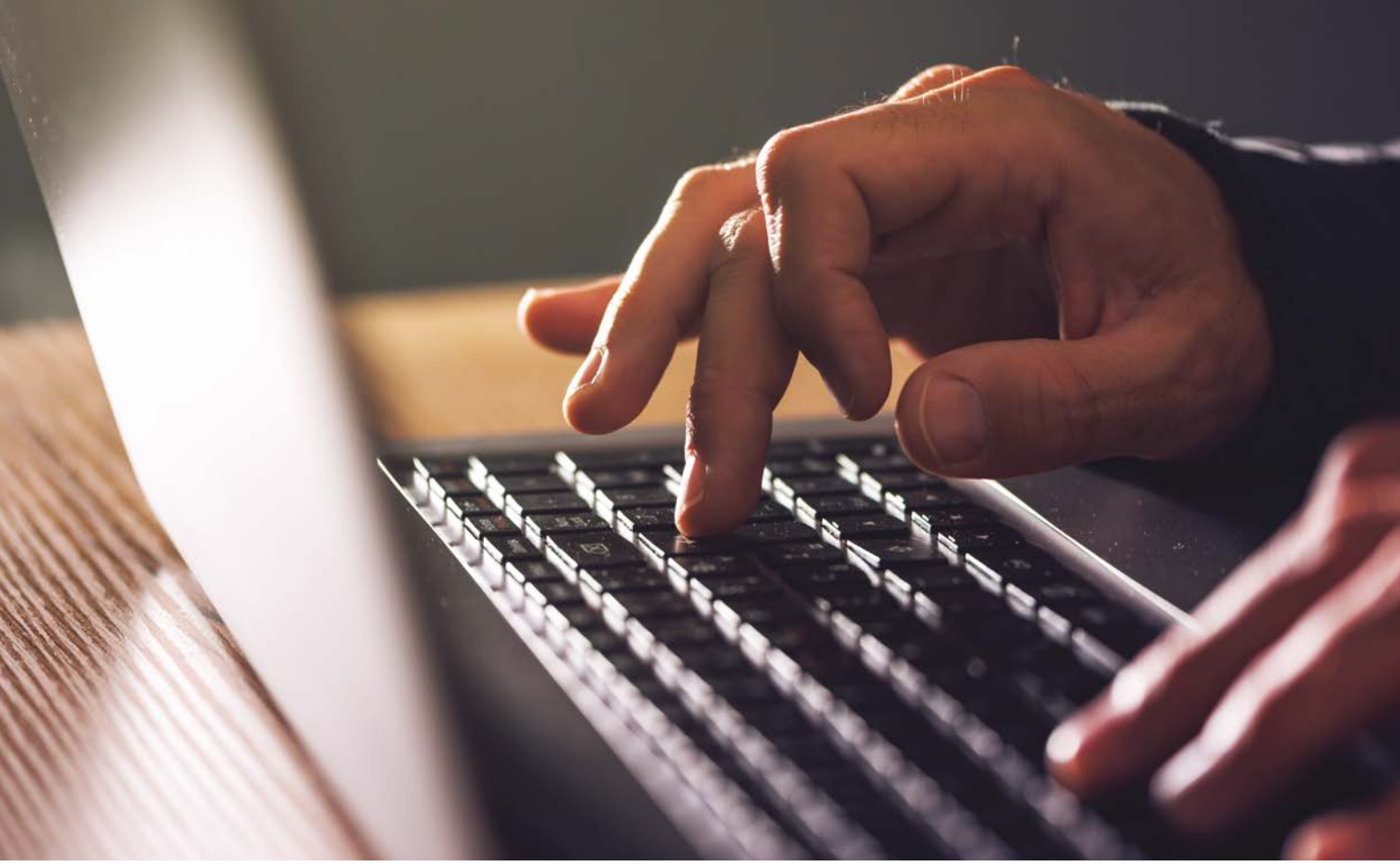
Unabhängig von ihrer Größe oder Branche waren Unternehmen, die in einer vernetzten und zunehmend digitalisierten Welt operieren, noch nie verwundbarer gegenüber Angriffen und den möglicherweise fatalen finanziellen Folgen, die daraus resultieren, als zum jetzigen Zeitpunkt. AIG erwartet, dass die 2017 beobachtete systemische Art von Ransomware-Angriffen nur die Spitze des Eisberges ist – in Zukunft warten noch größere Herausforderungen auf uns.

Da Prävention immer besser ist, als bereits entstandenen Schaden zu beheben, müssen sich Unternehmen auf eine unvermeidliche Verletzung ihrer Systeme und Netzwerke vorbereiten. Cyber-resiliente Unternehmen wappnen sich, proben den Ernstfall und führen eine adäquate, belastbare Cyber-Risikostrategie ein, mit der sie sicherstellen, dass sie gegen die gesamte Bandbreite von Cyber-Gefahren, einschließlich Netzwerkunterbrechung, geschützt sind.

Wichtige Cyber-Sicherheitsrisiken für Unternehmen

Mit Blick auf unsere Schadenerfahrung sind – in Bezug auf Sicherheitsprobleme – die wichtigsten Risiken für Unternehmen folgende:

- **Externe Server mit Remote-Zugriff in Verbindung mit schwachen Passwörtern, über die Schadsoftware und Ransomware eingeschleust werden.** Ein Remote-Zugriff sollte daher sorgfältig kontrolliert werden.
- **Mangelnde Vorsicht durch Nutzer, die das Hacking durch Passwort-Phishing ermöglicht.** Nutzer werden über eine Phishing-Mail zu einer gefälschten Login-Seite geleitet, auf der Anmeldedaten abgegriffen werden und die Accounts der Opfer für Hacker zugänglich werden. Nutzer sollten sich die Frage stellen, ob sie der E-Mail vertrauen. Bei jeglichen Abfragen von Login-Daten sollte an Phishing gedacht werden.
- **Schwache Login-Protokolle.** Das Risiko für Phishing entfällt, wenn eine Zwei-Faktor-Authentifizierung ermöglicht wird. Hierzu wird ein zweiter Code zum Account-Login benötigt. Zumindest für Geschäftsführer, Geschäftspartner und Mitarbeiter, die in Zahlungen involviert sind, sollte dies eingeführt werden.



Fallstudien zu Cyber-Schäden

Geschäftsunterbrechung nach einem Ransomware-Angriff bei einem Produktionsunternehmen

Der Versicherungsnehmer entwirft und fertigt Kräne, Bagger und schwere Spezialhubgeräte.

Am 1. Dezember stellt der Versicherte fest, dass er Opfer eines Ransomware-Angriffs wurde. Bis zu 85 % seiner Ordner und Dokumente wurden verschlüsselt. Der Versicherte wendet sich an die AIG CyberEdge-Hotline und erhält sofort Hilfe von einem IT-Forensikunternehmen. Aufgrund der Beratung entschied sich der Versicherte dafür, die Daten mit Hilfe von Backups wiederherzustellen. Diese Arbeit wurde bereits am 3. Dezember abgeschlossen.

Aufgrund des Ausfalls des IT-Systems konnten Mitarbeiter unterschiedlicher Abteilungen am 1. und 2. Dezember nicht arbeiten, da sie keinen Zugriff auf den Server hatten. Der Versicherte beschäftigt etwa 300 Produktionsmitarbeiter und Ingenieure. Sein Hauptgeschäft besteht aus schlüsselfertigen Projekten oder Ingenieurprojekten, für welche die Nutzung der IT-Infrastruktur zur Ausführung der Arbeit wesentlich ist.

Das Ingenieurteam speichert Daten auf dem Unternehmensserver, um diese mit anderen Mitarbeitern zu teilen. Die Ingenieurmitarbeiter stellen ihre Arbeitsstunden direkt einem Projekt in Rechnung. Die Tatsache, dass die Ingenieure während dieser zwei Tage nicht arbeiten konnten, wirkte sich also direkt auf die Anzahl der Stunden aus, die das Unternehmen in Rechnung stellen konnte. Das Nachholen dieser Arbeitsstunden zu einem späteren Zeitpunkt war schwierig, da der Versicherte bei seinen diversen Projekten Fristen einhalten musste. Hätte er diese versäumt, hätten seine Kunden Vertragsstrafen geltend gemacht.

Durch die Versicherung wurden die Zusatzkosten für Ingenieurmitarbeiter gedeckt, sodass die Fortführung der Arbeiten und der rechtzeitige Abschluss der Projekte sichergestellt werden konnte.

Androhung eines DDoS-Angriffs und Erpressung gegenüber einem Finanzinstitut

Das versicherte Finanzinstitut erhielt eine E-Mail mit einer Lösegeldforderung von einem Bitcoin und der Androhung eines DDoS-Angriffs. Weiterhin wurde gedroht, das Lösegeld auf zehn Bitcoins zu erhöhen, falls keine Zahlung erfolgen sollte.

Mit Hilfe von AIG beauftragte der Versicherungsnehmer einen DDoS-Schutzservice, um die Auswirkungen eines eventuellen Angriffs abzuschwächen und informierte seinen Internetanbieter über einen potenziellen Angriff. Er versuchte nicht, die Situation mit ungeeigneten Mitteln wie Firewalls selbst in den Griff zu bekommen.

Die Untersuchung des Vorfalls legte nahe, dass der vermeintliche Angreifer seinen Sitz in Lettland hatte. Er gab sich als „XMR Squad" aus, der Name einer Gruppe, die bereits in der Woche zuvor DDoS-Angriffe gegen mehrere Unternehmen durchgeführt hatte. Scheinbar handelte es sich also um eine glaubwürdige Bedrohung. Informationen der Bank of England legten jedoch nahe, dass die E-Mail möglicherweise von einem Trittbrettfahrer und nicht von der offiziellen Gruppe stammte.

Es gab keine Hinweise darauf, dass der angehende Angreifer Zugriff auf personenbezogene Daten erlangt hatte, die vom Versicherten gespeichert wurden. Die Drohung wurde letztendlich nicht umgesetzt, und die Vertraulichkeit, Integrität oder Verfügbarkeit der Datenbestände des Versicherten wurden nicht negativ beeinträchtigt.

Sowohl die Webseite als auch die digitale Plattform des Versicherungsnehmers blieben online und konnten genutzt werden, wenn auch mit erhöhter und fortlaufender Kontrolle und Traffic-Analyse. Das Finanzinstitut erlitt keinen ernsthaften finanziellen Schaden – abgesehen von den Kosten, die für externe Rechtsberatung und sonstige Krisenmanagement-Beratung in Zusammenhang mit dem Vorfall entstanden sind und den tatsächlich beachtlichen Zeitressourcen, die zur Untersuchung und Lösung des Vorfalls aufgebracht werden mussten. Die Kosten der Vorfallreaktion hat AIG übernommen.

Gezielter Phishing-Angriff auf ein Luxuswarenunternehmen

Das versicherte Unternehmen schien Opfer von Betrug durch Phishing-Mails zu sein, die zunächst die Mitarbeiter und später die Kunden erhielten.

Eine erste Untersuchung des Vorfalls zeigte, dass ein Mitarbeiter neun Monate vor Auftreten der Probleme auf einen Link in einer Phishing-Mail geklickt hatte und so sein Postfach für die Eindringlinge öffnete. Mindestens zwei weitere Postfächer von Mitarbeitern, die auf Links in ähnlichen Phishing-Mails geklickt hatten, waren betroffen. Durch Zugriff auf diese drei Postfächer ist es den Eindringlingen vermutlich gelungen, an die Kontaktdaten von Kunden zu gelangen.

Daraufhin erreichten den Versicherten über einen Zeitraum von 12 Monaten und mit steigender Häufigkeit Anfragen von Kunden, die gefälschte E-Mails erhalten hatten, welche vom Versicherten zu stammen schienen, tatsächlich aber von Betrügern versandt wurden. Diese E-Mails verleiteten die Kunden dazu, ebenso wie die ursprünglich an die Mitarbeiter versandte, auf einen falschen Link zu klicken. Anschließend wurden die Eingabe von Login-Daten, Kreditkarteninformationen und sonstigen personenbezogenen Daten, wie sie der Versicherte zur Kundenanalyse verwendet, gefordert.

Mehrere Kunden, die die Phishing-Mail meldeten, waren in einer Tabelle, die im E-Mail-Postfach eines Mitarbeiters gefunden wurde, aufgelistet. Insgesamt enthielt diese etwa 21.000 E-Mail-Adressen.

Forensische IT-Experten, die auf Anraten von AIG hinzugezogen wurden, blockierten den Zugriff auf die verdächtigte URL und führten eine zielgerichtete Untersuchung der betroffenen Postfächer durch, um festzustellen, auf welche Daten zugegriffen wurde. Nach einer umfangreichen Analyse wurde die Datenkompromittierung auf weniger als 1.000 Datensätze eingegrenzt. Schlussendlich handelte es sich bei den betroffenen Kunden häufig um vermögende und bekannte Persönlichkeiten, für die der Versicherungsnehmer im Anschluss maßgeschneiderte und personalisierte Antworten erstellen konnte.

DIE ANSPRÜCHE UNSERER VERSICHERTEN STEHEN AN ERSTER STELLE

Vorgehensweise

Im März 2018 führte AIG Europe eine Analyse von mehr als 600 Schadenfällen durch, welche von 2013 bis Dezember 2017 im Rahmen von Cyber-Policen gemeldet wurden.

Hinweis: Eventuelle Diskrepanzen der Prozentangaben, die im Vergleich mit dem AIG Schadenreport 2017 festzustellen sind, gründen auf potenziellen Verschiebungen in den absoluten Schadenzahlen durch u. a. nicht substantiierte Schadenfälle bzw. Fehlmeldungen.

www.aig.com

Nepomuk Loesti
Head of Financial Lines Europe
Tel: +49 (0) 69 97 113 271
nepomuk.loesti@aig.com

Oliver Delvos
Senior Underwriter und Teamleiter Cyber, DACH
Tel: +49 (0) 69 97 113 477
oliver.delvos@aig.com

Michael Unglaub
Manager Financial Lines Claims, DACH
Tel: +49 (0) 69 97 113 380
michael.unglaub@aig.com

Sebastian Hess
Cyber Risk Engineer, DACH
Tel: +49 (0) 69 97 113 572
sebastian.hess@aig.com

DEL00002801 09/18