Claims Intelligence Series

Der große Hintergrundbericht: DSGVO und Business E-Mail Compromise lassen Cyber-Schäden hochschnellen

Business E-Mail Compromise (BEC) überholt zum ersten Mal Ransomware und Datenschutzverletzungen als Ursache von Cyber-Schäden, so der aktuelle AIG EMEA[1] Cyber-Schadenreport. Nahezu ein Viertel der gemeldeten Schäden aus dem Jahr 2018 ließ sich demnach auf Business E-Mail Compromise zurückführen. Im Vergleich zum Vorjahr (2017) bedeutet dies einen Anstieg um 11 %. Ransomware, Datenschutzverletzungen durch Hacker und durch Fahrlässigkeit von Mitarbeitern sind dem Bericht zufolge die anderen hauptsächlichen Ursachen von Cyber-Sicherheitsvorfällen.

BEC[2] hat in diesem Jahr unter einer neuen Kategorie Eingang in den Bericht gefunden, zurückzuführen auf die hohe Anzahl an BEC-Vorfällen, die in den letzten 12 Monaten bei AIG gemeldet wurden.

In den meisten Fällen ging die Gefährdung von einer Phishing-E-Mail aus, die einen Link oder Anhang enthielt. Wenn der Empfänger den Inhalt einer Phishing-E-Mail nicht erkennt und die verlinkten Objekte anklickt, ermöglicht er den Hackern das Eindringen in den Posteingang des Benutzers. Die meisten Benutzer kennen zwar die Gefahr, die von Phishing-E-Mails ausgeht, aber es gibt immer noch viele Benutzer, die einem Link folgen, der den Empfänger zu einer gefälschten Anmeldeseite führt. Sobald das Opfer seine Anmeldedaten eingibt, werden sie vom Cyber-Kriminellen erfasst, sodass dieser sich dann problemlos beim E-Mail-Konto des Opfers anmelden kann.

Der Täter kann dann E-Mails mit der E-Mail-Adresse des Opfers senden und empfangen und auf alle Informationen im E-Mail-Posteingang des Opfers zugreifen. In vielen Fällen wird die BEC durch Schadsoftware verschärft, die versucht, weitere Kontakte aus dem Posteingang des Empfängers in den Betrug zu involvieren. BEC-Angreifer fokussieren beispielsweise häufig Einzelpersonen, die für die Überweisung von Zahlungen verantwortlich sind, mittels gefälschter Konten, indem sie sich als Führungskraft eines Unternehmens oder als Lieferant ausgeben und Überweisungen, Steuerunterlagen und/oder sonstige sensible Daten verlangen.

Abb. 1 **Cyber-Schadenmeldungen bei AIG EMEA (2018) – nach Ursache**

*Denial-of-Service-Angriffe, rechtliche/regulatorische Verfahren durch Verstöße gegen Datenschutzvorschriften

Auf einen Blick

- Business E-Mail Compromise ist nun die häufigste Ursache für Schäden durch Cyber-Angriffe, gefolgt von Ransomware, die zunehmend zielgerichtet und geschäftsschädigend ist und Betriebsunterbrechungskosten mit sich bringt. Die Folgen von Cyber-Angriffen werden weiterhin stark von menschlichem Versagen beeinflusst.
- Die Branche für Professionelle Dienstleistungen (z. B. Architekten, Rechtsberatung, Makler etc.) ist inzwischen am häufigsten von Cyber-Angriffen betroffen. Gleich darauf folgt der Bereich der Finanzdienstleistungen. Cyber-Vorfälle verteilen sich jedoch auf alle Branchen, was zeigt, dass keine Branche gegen Cyber-Angriffe immun ist.
- Der Trend einer steigenden Häufigkeit von Cyber-Vorfällen setzt sich auch 2018 weiter fort. Insgesamt wurden im vergangenen Jahr genauso viele Vorfälle gemeldet wie in den beiden vorangegangenen Jahren zusammen.

Methodik

Zwischen 2013 und Dezember 2018 führte AIG eine Analyse bei mehr als 1.100 EMEA-Cyber-Schäden durch. Die Ergebnisse dieser Analyse geben einen allgemeinen Einblick nur für diesen Bereich. Insofern gilt es zu berücksichtigen, dass auch andere Industriezweige und Branchen von zahlreichen und schwerwiegenden Schäden betroffen gewesen sein können. In 2018 entsprach die Zahl der AIG gemeldeten Cyber-Schäden im Großen und Ganzen dem Prämienwachstum für dieses Produkt.

[1] Europa, Middle East & Afrika
[2] Zuvor fielen solche Angriffe unter den Bereich „Sonstige Sicherheitsprobleme/unberechtigte Zugriffe".

Andere Attacken konzentrieren sich auf den Inhalt im Posteingang des Empfängers, um Kunden- und Mitarbeiterdaten einschließlich personenbezogener Daten zu erlangen. Sie können auch auf vertrauliche Unternehmensinformationen abzielen wie zum Beispiel Geschäftsgeheimnisse. Die meisten sind jedoch durch finanziellen Gewinn motiviert.

„Letztlich steckt hinter vielen dieser Angriffe organisiertes Verbrechen", so Jonathan Ball, Partner bei Norton Rose Fulbright. „Sie sind nicht daran interessiert, personenbezogene Daten zu stehlen und sie im Darknet zu verkaufen. Es ist rein finanzieller Betrug."

BEC-Angriffe sind häufig erfolgreich, weil sie mithilfe von Techniken aus dem Social-Engineering E-Mails erstellen, die rechtmäßig aussehen. Selbst größere Unternehmen können auf Betrug hereinfallen, erklärt Jose Martinez, Vice President of Financial Lines Major Loss Claims bei AIG, EMEA. Er empfiehlt, mehr in die Schulung der Mitarbeiter zu investieren, damit sie gefälschte E-Mails besser erkennen. „Wir sehen immer noch ein überraschend hohes Ausmaß dieser Betrugsarten – selbst bei sehr großen Unternehmen. Man könnte meinen, dass jeder Finanzvorstand eines großen Unternehmen inzwischen davon gehört haben sollte, aber es geschieht immer noch."

Die Cyber-Police bietet Schutz bei Business E-Mail Compromise und Identitätsbetrug und übernimmt die Kosten für eine IT-forensische Untersuchung, um festzustellen, ob das System des Versicherungsnehmers infiziert wurde, und die entsprechenden Daten zu identifizieren. Sie umfasst auch die Kosten für die Rechtsberatung in Bezug auf die Melde- und Benachrichtigungspflichten gegenüber betroffenen Personen und Aufsichtsbehörden, obwohl der Versicherungsschutz für finanzielle Verluste durch kriminelle Aktivitäten oft eingeschränkt ist.

„Die Untersuchungen dieser Vorfälle werden immer teurer", erklärt Mark Camillo, Leiter Cyber für EMEA bei AIG. „Wenn sich ein Angreifer Zugriff auf die Mailbox verschafft hat, muss gründlich untersucht werden, auf welche Informationen er möglicherweise Zugriff hat und ob dadurch die DSGVO-Vorschriften verletzt wurden."

Obwohl Finanzdienstleistungsunternehmen die ersten Käufer von Cyber-Versicherungen waren und auch den größten Industriezweig bilden, lässt sich 2018 feststellen, dass die Zahl der gemeldeten Schäden bei Unternehmen des Dienstleistungssektors anstieg. Dieser Bereich ist auch am anfälligsten für Business E-Mail Compromise. Im Jahresvergleich stieg die Zahl der Schadenfälle in diesem Bereich einschließlich Anwaltskanzleien und Steuerberatern, von einem Jahr auf das nächste von 18 % auf 22 %.

Abb. 2 **Cyber-Schadenmeldungen bei AIG EMEA (2018) – nach Branche**

*Nahrungsmittel und Getränke, Bauwesen, Bildung

Hinweis: Aufgrund rundungsbedingter Abweichungen ergeben die Werte möglicherweise keine 100 %

Camillo ist der Meinung, dass solche Unternehmen aufgrund von mangelnder Erfahrung beim Thema Cyber-Sicherheit anfälliger für BEC sein könnten. „Die Kriminellen gehen dorthin, wo sie das meiste Geld machen können", sagt er. „Da Unternehmen im Finanzdienstleistungsbereich einer starken Regulierung unterliegen, haben diese tendenziell bessere Kontrollen als Unternehmen anderer Branchen. Dies umfasst auch die Professionellen Dienstleistungen, z. B. Architekten, Rechtsberatung, Makler etc."

Er geht davon aus, dass mit Inkrafttreten des überarbeiteten technischen Standards im Rahmen der Zahlungsdiensterichtlinie (Payment Services Directive, PSD2) die Häufigkeit von BEC-Angriffen möglicherweise sinkt. Gemäß der Richtlinie müssen Zahlungsdienstleister die Anforderungen für eine starke Kundenauthentifizierung (Strong Customer Authentication, SCA) und den Zugriff Dritter auf Bankkonten erfüllen, was Betrügern das Stehlen und Umleiten von Geldern erschweren dürfte.

Schlechte Passworthygiene ist ein immer wiederkehrendes Problem für Unternehmen, die von BEC betroffen sind. Cyber-Kriminelle nutzen die Unternehmen aus, die bei den Microsoft Office 365 Standardeinstellungen nicht alle erforderlichen Sicherheitsfunktionen, wie die Multi-Faktor-Authentifizierung, aktiviert haben. Das ist nach wie vor ein äußerst häufiger Vorfall, der laut Kathy Avery, Financial Lines Major Loss Adjuster, AIG, fast täglich dem AIG Cyber-Schadenteam gemeldet wird.

„Für Unternehmen, die von BEC betroffen sind, kann dies einen großen Reputationsschaden bedeuten", fährt sie fort. „Für viele Unternehmen stellt die Benachrichtigung ihrer Kunden nach einem Angriff eine große Hürde dar. Und oft stellen sie den Angriff nur fest, weil ihre Kunden Spoofing- und Phishing-E-Mails erhalten, die scheinbar vom Versicherungsnehmer stammen und eine Folge des BEC sind."

Die Sicherheitsbedenken rund um Passwörter und Multi-Faktor-Authentifizierung sind ernst zu nehmen. Dennoch bleibt es eine Tatsache, dass viele einfache Angriffe verhindert werden könnten, indem das Bewusstsein der Mitarbeiter für Phishing-E-Mails verbessert und ein klarer Prozess für den Umgang mit verdächtigen E-Mails implementiert werden.

Das Segment der Finanzdienstleistungen ist heute der zweite Bereich, der für die meisten Cyber-Schadenmeldungen verantwortlich ist. Nach dem bisherigen Spitzenplatz ist dieser Bereich im Jahr 2018 für 15 % der Schadenfälle verantwortlich, nach 18 % im Vorjahr. Die Prozentsätze spiegeln jedoch nicht die gesamte Entwicklung wider. Tatsächlich hat sich die Gesamtzahl der Schadenmeldungen von Finanzdienstleistern zwischen 2017 und 2018 sogar nahezu verdoppelt. Dies zeigt, dass die Branche trotz ihres höheren Schutzniveaus bei Cyber-Risiken immer noch ein häufiges Ziel ist.

Gleiches gilt für das Hotel-, Gaststätten- und Freizeitgewerbe. Die Zahl der realen Schadenfälle hat sich im Jahr 2018 erneut nahezu verdoppelt, obwohl sie im Jahresvergleich von 5 % auf 4 % zurückgegangen ist. „Wir sehen viele Vorfälle im Zusammenhang mit Kundenbindungsprogrammen, wobei in der Regel Hotellerie und Gastronomie sowie Fluggesellschaften betroffen sind", sagt Ball. „Viele der Handelsmarken aus dem Hotel- und Gastronomiegewerbe sind Franchise-Unternehmen. Sie teilen ihre Kunden- und Buchungsdaten und oft können weltweit alle im Hotelverbund auf diese Daten zugreifen."

Der Faktor Mensch

Menschliches Versagen und Verhaltensweisen sind nach wie vor wesentliche Treiber für Cyber-Schäden. Entgegen der Empfehlung vieler Unternehmen verwenden Mitarbeiter oft schwache Passwörter oder dieselben Passwörter für mehrere Anwendungen.

„Ein Unternehmen, das wir versichern, hat einen Angriff auf seine Systeme vereitelt, nachdem es einen Angreifer in seinem System festgestellt hat", sagt Kathy Avery in London. „Das Unternehmen beschloss, alle Passwörter zurückzusetzen und bat alle Mitarbeiter, neue Passwörter anzulegen. Dennoch konnte es den Eindringling nicht loswerden. Erst der zweite Versuch mit zufällig generierten Passwörtern für jeden Benutzer war erfolgreich und man schaffte es schließlich, den Zugriff zu unterbinden."

Im diesjährigen AIG Schadenreport haben sich die Schadenmeldungen wegen Fahrlässigkeit von Mitarbeitern von 7 % auf 14 % verdoppelt. Die Schäden werden dadurch ausgelöst, dass Mitarbeiter E-Mails mit Unternehmensdaten an falsche Adressaten senden oder Laptops und andere technische Geräte verlieren. Außerdem hat seit Inkrafttreten der DSGVO die Zahl der Meldungen solcher Vorfälle zugenommen.

„Wir beobachten, dass z. B. Anhänge vor dem Versenden an E-Mails oft nicht überprüft werden. Der Absender denkt, dass er nur einen einzelnen vertraulichen Satz personenbezogener Daten verschickt, versehentlich aber eine viel größere Menge vertraulicher personenbezogener Datensätze versendet", sagt Jonathan Ball.

Ein weiterer typischer Fehler tritt bei der Anwendung von Excel-Tabellen auf. „Viele Mitarbeiter verstehen die Funktionsweise von Excel nicht. So kommt es zum Beispiel vor, dass sie die Filter-Schaltfläche aktiviert haben und daher nur bestimmte Daten im Arbeitsblatt auf ihrem Bildschirm sehen", sagt Ball. „Wenn sie dann das Dokument versenden, ohne die Filterfunktion wieder zu deaktivieren, kann der Empfänger ganz leicht viele weitere Daten sehen. Wir haben vor kurzem einen derartigen großen Sicherheitsvorfall bei einer Bank behandelt."

Es gibt viele Nachlässigkeiten und Fehler, die sich nach wie vor unverändert einschleichen", fährt er fort. „Die Leute klicken immer noch ständig auf Phishing-E-Mails, trotz Schulung. Und eines der Dinge, die die Kosten für die Behandlung von Schadenfällen wirklich in die Höhe treiben, ist die Nutzung der Firmen-E-Mail durch Mitarbeiter für private Angelegenheiten, insbesondere für private Finanzangelegenheiten. Zusätzlich steigen die Kosten für notwendige Meldungen an die zuständigen Aufsichtsbehörden und die Benachrichtigung der Betroffenen.

Anstieg gezielter Ransomware

In 2017 führten Cyber-Schäden durch Ransomware mit 26 % aller Schadenmeldungen die Statistik an. Die Zahl ist 2018 allerdings nur geringfügig auf 18 % zurückgegangen. Wie jedoch schon in der AIG Schadenstudie im letzten Jahr prognostiziert, zeigt sich, dass Ransomware- und Erpressungsangriffe gezielter werden, wobei der Angriff auf einen internationalen Aluminiumproduzenten in Norwegen eines der bekannteren Beispiele ist.

Das Unternehmen wurde Opfer eines schwer zu entdeckenden Ransomware-Angriffs, der als „LockerGoga" bekannt ist. Cyber-Kriminelle erhielten damit Zugriff auf die Netzwerke des Unternehmens. Das Unternehmen war gezwungen, die Produktion in mehreren Werken in Europa und den USA zu stoppen und auf manuelle Abläufe umzustellen, um das Problem einzudämmen. Weitreichende Betriebsunterbrechungen waren die Folge.

Die Entscheidung, ob eine Lösegeldforderung oder Erpressungsgeld bezahlt werden muss, hängt weiterhin sowohl davon ab, wie gut eine Organisation ihre Daten gesichert hat, als auch von dem erwarteten Umfang einer möglichen Betriebsunterbrechung. „Die Auswirkungen von Ransomware können erheblich gemildert werden, wenn es bewährte Prozesse für die Datensicherung durch Backups gibt", so Avery. „Leider ist dies aber nicht überall gewährleistet."

In der Zwischenzeit hat die Höhe der Lösegeldforderungen zugenommen. Die anfänglichen Beträge, die von WannaCry-Ransomware-Angreifern gefordert wurden, lagen zwischen 300 und 600 US-Dollar. Dahingegen gab es im Jahr 2018 Fälle, bei denen Cyber-Kriminelle Zehntausende von Dollar, Euro oder Bitcoin forderten. Unterdessen sind die mit solchen Angriffen verbundenen Kosten für Betriebsstörungen und -unterbrechungen gestiegen. Und in Zeiten der DSGVO besteht außerdem die Notwendigkeit festzustellen, ob sensible Daten gefährdet wurden.

"2018 haben wir mehr Cyber-Erpressungen gesehen. Auch sind die Kosten für die Wiederherstellung der Systeme gestiegen", so Camillo. „Selbst wenn man Lösegeld zahlt, um die Dateien zu entschlüsseln, ist es ein sehr aufwendiges Verfahren. Denn man muss erneut überprüfen, ob die Entschlüsselung funktioniert und muss dann die Daten isolieren, um sicherzustellen, dass sie nicht erneut infiziert werden. Außerdem müssen alle Dateien bereinigt werden, bevor man alles neu installiert. Das ist sehr teuer und stört den Unternehmensablauf enorm und sollte nur als letztes Mittel eingesetzt werden, dort wo es gesetzlich zulässig ist."

Er geht davon aus, dass die Zahl der Schadenansprüche durch Cyber-Angriffe aufgrund von Betriebsunterbrechungen weiterhin stark steigen wird, da Lösegeld- und Erpressungsangriffe gezielter werden. Hinzu kommt, dass Versicherungsnehmer ihren Versicherungsschutz besser kennen.

„Wir erwarten einen Anstieg der Schadenfälle auf globaler Ebene", sagt Camillo. „Gezielte Vorfälle, wie der Angriff auf den norwegischen Aluminiumkonzern, könnten 2019 ein größeres Problem werden. Die schnelle Ausbreitung von Schadsoftware oder der Angriff auf einen kritischen Dienstleister durch staatlich geförderte Akteure könnte zu weitreichenden Betriebsunterbrechungen führen und eine Vielzahl von Branchen betreffen, und möglicherweise auch erhebliche Sachschäden verursachen."

Schadenhäufigkeit und DSGVO-Effekt

In 2018 gab es im Hinblick auf die Schadenfrequenz einen ausgeprägten „DSGVO-Effekt“, mit einem sprunghaften Anstieg der Meldungen nach Inkrafttreten der EU-Datenschutz-Grundverordnung im Mai 2018. Die neuen Vorschriften und strengen Richtlinien zur Meldung von Datenschutzverletzungen führt zu rechtzeitigen Benachrichtigungen der Kunden.

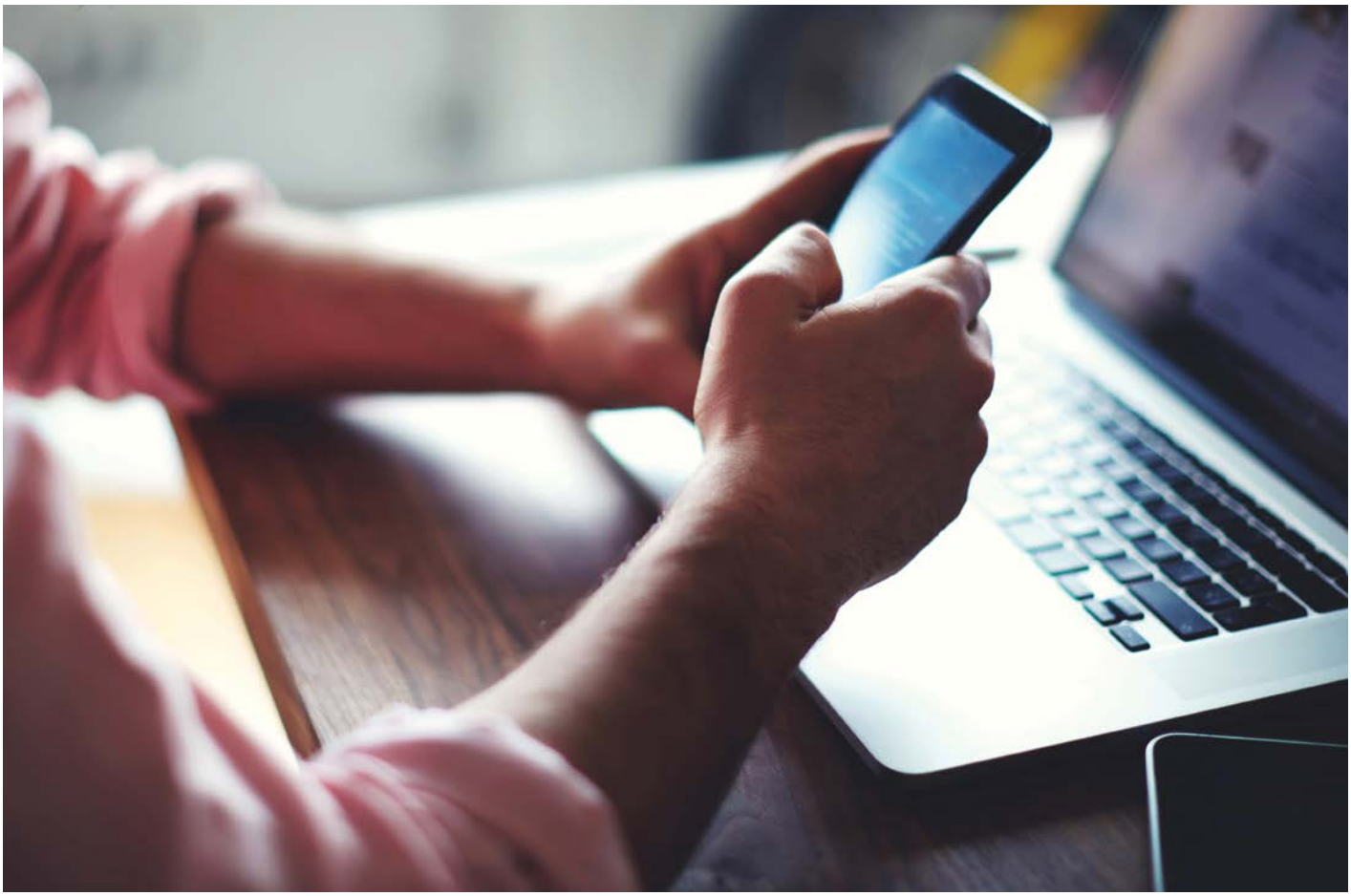
„Es gibt eine sehr strenge Frist, vor allem was die Meldung an die Aufsichtsbehörde betrifft. Das hat einen Anstieg der Anfangskosten zur Folge“, sagt Avery. „In unserer Versicherungspolice bieten wir einen 48- oder 72-stündigen Zeitraum, in dem wir die Anfangskosten tragen. Für diesen Zeitraum stellen wir eine erhöhte Schadenaktivität fest. Darüber hinaus sind die Kosten für Rechtsberatung, Forensik und IT gestiegen, was zu höheren Auszahlungen im Rahmen der Police führt.“

Knapp 20 % der bei der AIG im Jahr 2018 eingegangenen Schadenmeldungen beinhalteten eine DSGVO-Meldung, wobei die Kosten im Vergleich zu Schadenfällen, bei denen es keine Meldung über eine Datenschutzverletzung gab, wesentlich höher waren. Die Schadenaktivitäten aus unserer Notruf-Hotline haben bei Schadenfällen, bei denen die betroffenen Personen und/oder die Datenbehörde benachrichtigt wurde, um über 50 % zugenommen, wobei die Versicherungsnehmer rechtliche Beratung und Unterstützung bei der Vorbereitung ihrer aufsichtsrechtlichen Meldungen erhalten haben.

„Wir sehen auf unsere Kanzlei viel Arbeit zukommen und auch höhere Gebühren für Versicherungsnehmer und/oder Versicherer für die Bearbeitung von DSGVO-Verstößen, selbst bei wirklich sehr geringfügigen Datenschutzverletzungen“, sagt Jonathan Ball von Norton Rose Fulbright. „Kleinere Verstöße hätte vor der DSGVO ein Unternehmen wohl allein ohne externe Rechtsanwälte behandelt.“

In Europa gibt es bei den Meldungen über DSGVO-Datenschutzverletzungen ein klares Nord-Süd-Gefälle, wobei Nordeuropa für die überwiegende Mehrheit der Meldungen verantwortlich ist. Dies deutet auf eine unterschiedliche Compliance-Kultur hin. Beispielsweise führten in Irland 48 % der gemeldeten Vorfälle zu einer Meldung an eine Aufsichtsbehörde, während in Spanien weniger als 10 % der Vorfälle gemeldet wurden. Die DSGVO kann auch für Kunden gelten, die in Ländern außerhalb Europas ansässig sind. Dies wird durch eine Zunahme der Meldungen aus dem Nahen Osten und Afrika bestätigt. Hier gab es in den letzten 12 Monaten mehr Schäden.

Betrachtet man die Cyber-Statistiken nach Regionen so zeigt sich, dass die Meldungen aus Belgien, den Niederlanden, Deutschland, Frankreich und Irland in den letzten 12 Monaten deutlich zugenommen haben, ebenso wie die Anzahl der gemeldeten Schäden aus Schweden und Griechenland.



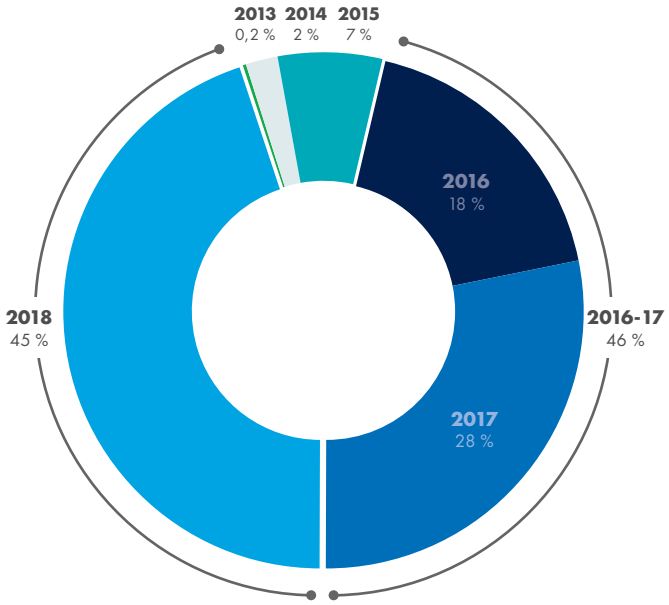
Vorausschauend: Tendenz in Richtung explizitem Versicherungsschutz

Der langfristige Trend einer zunehmenden Schadenhäufigkeit hat sich auch 2018 wie in den letzten fünf Jahren fortgesetzt, was sowohl das Wachstum als auch die Reife des AIG Cyber-Portfolios als auch die zunehmende Sensibilisierung von Käufern und das bessere Wissen über den Umfang des Produktes widerspiegelt. Da Cyber für viele Unternehmen zu einem immer größeren Risiko wird, werden die erwarteten Schäden unserer Erfahrung nach sowohl in der Häufigkeit als auch in der Schwere über verschiedene Branchen hinweg weiter zunehmen.

Camillo stellt eine fortgesetzte Tendenz in Richtung explizitem Versicherungsschutz bei Kunden fest, die sicherstellen wollen, dass ihre Versicherungspolice den erwarteten Schutz bietet. „Es gab in der letzten Zeit in der Presse einige Fehleinschätzungen über den Cyber-Versicherungsschutz."

„Was unsere Schadenzahlen deutlich zeigen ist, dass mehr Menschen die Deckung kaufen und das Produkt sich am Bedarf unserer Kunden orientiert", fährt er fort. „Es umfasst einen sehr breiten und flexiblen Versicherungsschutz und es ist sehr einfach, uns über die Hotline über einen Vorfall zu informieren. Kunden bevorzugen den expliziten Cyber-Versicherungsschutz, der eine große Bandbreite von Schäden abdeckt, darunter Datenschutzverletzungen, Cyber-Erpressung und Netzwerkunterbrechungen einschließlich externer Dienstleister und Systemausfälle."

Abb. 3 **Cyber-Schadenmeldungen bei AIG EMEA (2013 - 2018) – nach Volumen**



Fallstudien zu Cyber-Schäden*

Hersteller erleidet Betriebsunterbrechung

Ein Angriff auf die IT-Systeme des versicherten Unternehmens erfolgte durch ein schädliches Ransomware-Programm, bekannt als „Detractor". Drei Server der IT-Infrastruktur waren betroffen, was zur Verschlüsselung der Dateien führte. Die verfügbaren Sicherungskopien, die sich auf einem anderen Server befanden, wurden gelöscht - vermutlich von den Cyber-Kriminellen. Daher konnten die betroffenen Systeme nicht durch die Sicherungskopien wiederhergestellt werden.

Gleichzeitig forderten die Cyber-Kriminellen, dass das versicherte Unternehmen ein Lösegeld zahlt, um das System zu entschlüsseln. Der Betrieb des Unternehmens war zum Erliegen gekommen, weil er die betroffenen Systeme nicht wiederherstellen konnte. Das Unternehmen konnte keine Lieferungen versenden oder Materialien empfangen und war nicht in der Lage, Zahlungen zu tätigen oder Forderungen einzuziehen.

Das Ziel der Ransomware war nicht, Informationen zu stehlen, und es gab keinen Zugriff auf personenbezogene Daten. Am 10. Tag des Vorfalls konnte das System wiederhergestellt werden, und das Unternehmen konnte seine Geschäftstätigkeit wieder aufnehmen. AIG übernahm die Kosten für die Reaktion auf den Vorfall und für die umfangreiche Netzwerkunterbrechung, die auch erhöhte Kosten für laufende und stornierte Bestellungen umfasste.

E-Mail-Konto bei Finanzdienstleistungsvermittler kompromittiert

Der Versicherte, ein mittelständisches Dienstleistungsunternehmen, wurde von mehreren Kunden auf einen Cyber-Vorfall aufmerksam gemacht, die eine verdächtige E-Mail von einem Mitarbeiter des Unternehmens erhalten hatten. Die E-Mail enthielt verschiedene Links und eine angehängte PDF-Rechnung, die die Empfänger bezahlen sollten.

Erste Untersuchungen ergaben, dass das E-Mail-Konto des Mitarbeiters kompromittiert worden war und eine Phishing-E-Mail mit einer angehängten Rechnung an 5.500 E-Mail-Adressen gesendet worden war. Das betroffene Unternehmen ergriff proaktiv gegensteuernde Maßnahmen, indem er die 720 E-Mail-Kontakte des kompromittierten Kontos benachrichtigte und ihnen dringend riet, das PDF-Dokument nicht anzuklicken. Die Passwörter sowohl des kompromittierten E-Mail-Kontos als auch anderer Mitarbeiter der Firma wurden geändert.

AIG empfahl dem Unternehmen, vorsorglich die zuständige Datenschutzbehörde zu benachrichtigen, obwohl die einzigen identifizierbaren Informationen nur die Namen und Arbeitsorte der Empfänger waren. Der Empfehlung zugrunde lagen unter anderem die Art des Unternehmens, einschließlich Verkauf von Cyber-Versicherungsprodukten, und auch Reputationserwägungen.

*Die hier beschriebenen Szenarien dienen nur als Beispiele. Der Deckungsumfang der Versicherung unterliegt den Allgemeinen Bedingungen der Police.

Netzwerkverletzung eines globalen Energie- und Logistikunternehmens im Nahen Osten

Ende des letzten Jahres gab es bei einem versicherten Unternehmen mehrere Brute-Force-Angriffe auf die Netzwerkinfrastruktur. Cyber-Kriminelle erhielten, höchstwahrscheinlich über seinen E-Mail-Cloud-Host, Zugang zum Unternehmensnetzwerk. Die konkrete Angriffsmethode wird aktuell noch untersucht. Das Netzwerk des Unternehmens umfasst ca. 5.000 Endpunktgeräte. Nach der Entdeckung wurden bei einer ersten Analyse etwa 2.900 eventuell infizierte Einheiten identifiziert. Daraufhin waren alle Benutzer gezwungen, ihre Passwörter zu ändern. Anschließend führte man die Zwei-Faktoren-Authentifizierung ein.

Das versicherte Unternehmen wandte sich im Rahmen der 72-Stunden-Frist über die Notfall-Hotline an die AIG Dienstleister. Aufgrund staatlicher Vorgaben durfte das Unternehmen seine Daten nicht außerhalb des Landes bearbeiten lassen, so dass sich die IT-Forensik zunächst auf die Beratung per Telefon und E-Mail beschränken musste. AIG konnte jedoch ein Team aus externen Dienstleistern bereitstellen, das zusammen mit dem Unternehmen Ermittlungen vor Ort durchführte.

Zunächst ging es vor allem darum, kompromittierte Zugangsstellen zu identifizieren und diese für die Cyber-Kriminellen zu schließen. Nach der Identifizierung konnte mithilfe der Netzwerkanalyse festgestellt werden, wie die Angreifer Zugriff erhalten hatten. Dabei zeigte sich auch, dass die Angreifer möglicherweise Zugriff auf E-Mail-Konten und auf über 2.000 Dateien mit personenbezogenen Daten erhalten hatten, darunter auch vertrauliche Unternehmensdaten wie Angebotsdaten, Projektdetails und Finanzkennzahlen.

Auch sechs Monate später laufen immer noch die Untersuchungen im Hinblick auf eine mögliche Kompromittierung von E-Mail-Konten, ebenso wie die Untersuchung und Analyse der infizierten Daten. Dafür fallen weiterhin Kosten an und betragen derzeit über 300.000 US-Dollar.

Einzelhändler getroffen von Ransomware und Betriebsunterbrechung

Der Versicherungsnehmer ist ein internationaler Einzelhändler mit über 100 Filialen und einem Online-Shop. Der scheinbar gezielte, ausgeklügelte Cyber-Angriff erfolgte, während das Unternehmen einige Änderungen an den IT- und Datenspeichersystemen vornahm. Dabei wurden alle Dateien verschlüsselt, auch die, die in der Cloud gespeichert waren. Die Cyber-Kriminellen forderten Lösegeld für die Bereitstellung eines Entschlüsselungscodes.

AIG hat sofort unterstützt und Kontakt zu externen Dienstleistern hergestellt, die für einen längeren Zeitraum ununterbrochen vor Ort Beistand geleistet haben. Sie arbeiteten sofort an der Sicherung des Systems und versuchten, unverschlüsselte Daten abzurufen. Dies erwies sich als sehr schwierig und war nicht in einem Zeitrahmen zu erreichen, der die Wiederaufnahme des normalen Geschäftsbetriebs ermöglichte. Die Filialen konnten zwar weiterhin mit manuellen Kassen betrieben werden, aber es konnten die Bestände in den Geschäften nicht aufgefüllt und Online-Bestellungen nicht bearbeitet werden, was zu einer erheblichen Betriebsunterbrechung führte.

Zunächst wollte sich das Unternehmen nicht mit den Cyber-Kriminellen auseinandersetzen. Aber nachdem es sein Geschäft über längere Zeit nur stark eingeschränkt betreiben konnte, entschloss es sich doch, das verlangte Lösegeld von 150.000 US-Dollar in Bitcoin zu zahlen. Nachdem das Lösegeld bezahlt worden war, wurde der Entschlüsselungscode zur Verfügung gestellt, aber alle Dateien mussten manuell mit dem Code entschlüsselt werden - ein mühsamer und kostspieliger Prozess, der von AIG entsprechend der Versicherungspolice bezahlt wurde.

AIG übernahm auch die Kosten für die verschiedenen Softwareanbieter des Versicherten für zusätzliche Unterstützung und Ausrüstung, um den Entschlüsselungsprozess voranzutreiben. Die Deckung des Unternehmens belief sich auf 1 Mio. Pfund, was sich als unzureichend erwies. Die Versicherungssumme wurde ausgezahlt, als die Betriebsunterbrechungsschäden 550.000 Pfund überschritten. Allein die Kosten für die IT-Forensik überschritten 500.000 Pfund.

Wenngleich die IT-Untersuchung bestätigte, dass es keine Anhaltspunkte dafür gab, dass personenbezogene Daten abgerufen oder extrahiert worden waren, und auch die rechtliche Beratung feststellte, dass eine Mitteilung an das ICO nicht erforderlich sei, waren die Kosten für Rechts- und IT-Beratung entsprechend den Bedingungen der Police gedeckt.

DIE ANSPRÜCHE UNSERER VERSICHERTEN STEHEN AN ERSTER STELLE

www.aig.de

Nepomuk Loesti
Head of Financial Lines Europe
T +49 69 97113-271
nepomuk.loesti@aig.com

Michael Unglaub
Financial Lines Claims Manager DACH
T +49 69 97113-380
michael.unglaub@aig.com

José Martinez
VP Financial Lines Major Loss Claims EMEA
T +20765160711
jose.martinez@aig.com

Dieses Dokument behandelt nur Cyber-Schäden im Zusammenhang mit einem AIG Versicherungsprogramm. Das Vertrauen oder die Befolgung etwaiger in diesem Dokument enthaltenen Informationen, Vorschläge oder Empfehlungen garantiert keinesfalls die Erfüllung Ihrer sich aus Ihrer Versicherungspolice ergebenden Verpflichtungen bzw. solcher Verpflichtungen, die in sonstiger Weise möglicherweise in Gesetzen, Bestimmungen oder Vorschriften vorgesehen sind.

Der Zweck dieses Dokuments besteht allein darin, Informationen bereitzustellen, und Sie sollten nicht im Vertrauen auf die in diesem Dokument enthaltenen Informationen irgendwelche Maßnahmen treffen. Dieses Dokument ist kein Ersatz für Ihre eigenen Untersuchungen und die Einholung professioneller oder fachlicher Beratung. Es werden keine Gewährleistungen, Garantien oder Zusicherungen – weder ausdrücklich noch stillschweigend – bezüglich der Richtigkeit oder Angemessenheit der in diesem Dokument angeführten Zusagen geleistet. AIG übernimmt keine Haftung, wenn dieses Dokument für einen anderen als den vorgesehenen Zweck verwendet wird.

Die hier beschriebenen Szenarien werden nur als Beispiele angeboten. Die Deckung hängt vom jeweiligen Sachverhalt jedes Falls und den Bedingungen, Voraussetzungen und Ausschlüssen der jeweiligen Versicherungspolice ab. Jeder, der an den oben genannten Produkten interessiert ist, sollte eine Kopie der Police anfordern, um eine Beschreibung des Umfangs und der Beschränkungen der Deckung zu erhalten.

American International Group, Inc. (AIG) ist ein internationales Versicherungsunternehmen. Mit der Kompetenz und Erfahrung von 100 Jahren bieten AIG Gesellschaften heute eine große Bandbreite an Sach- und Unfallversicherungen, Lebensversicherungen, Altersvorsorgekonzepten und anderen Finanzdienstleistungen für Kunden in mehr als 80 Ländern und Jurisdiktionen. Zu unseren unterschiedlichen Angeboten gehören Produkte und Dienstleistungen, die Geschäfts- und Privatkunden dabei unterstützen, ihre Vermögenswerte zu schützen, sich gegen Risiken abzusichern und für das Alter vorzusorgen. Stammaktien von AIG sind an der Börse in New York notiert.

Weitere Informationen über AIG finden Sie unter www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig.

AIG ist der Marketingname für das weltweite Versicherungsgeschäft der American International Group, Inc., das Sach- und Unfallversicherungen, Lebensversicherungen, Altersvorsorgeprodukte und allgemeine Versicherungsprodukte umfasst. Weitere Informationen finden Sie auf unserer Website unter www.aig.com.

Alle Produkte und Dienstleistungen werden von Tochtergesellschaften oder verbundenen Unternehmen der American International Group, Inc. erbracht bzw. zur Verfügung gestellt. Produkte und Dienstleistungen sind möglicherweise nicht in allen Ländern und Jurisdiktionen verfügbar. Der Deckungsumfang der Versicherung ist abhängig von den Underwriting-Anforderungen und den jeweiligen Bedingungen der Police. Versicherungsfremde Produkte und Dienstleistungen können von unabhängigen Dritten zur Verfügung gestellt werden.

AIG Europe S.A. ist ein Versicherungsunternehmen eingetragen unter R.C.S. Luxembourg Nummer B 218806, mit Hauptsitz in 35D, Avenue John F. Kennedy, L-1855 Luxembourg.
Chairman of the Board der AIG Europe S.A.: Jean-Marie Nessi
Hauptbevollmächtigter der deutschen Niederlassung: Alexander Nagler
AIG Europe S.A., Direktion für Deutschland, eingetragen im Handelsregister des Amtsgerichts Frankfurt am Main unter HRB 112611, hat ihren Sitz in Neue Mainzer Straße 46 – 50, 60311 Frankfurt, Deutschland, T +49 69 97113-0.

DEL00003606 1019