AIG

Claims Intelligence Series

Der große Hintergrundbericht: Die Ursachen von Schadenfällen in der Cyber-Versicherung

Cyber-Erpressung und Ransomware haben als Ursache für Cyber-Schäden in Klein- und Großunternehmen stark zugenommen, wie der europäische Datenreport von AIG zu Schadenfällen in der Cyber-Versicherung belegt. Weiterhin sind Datenschutzverletzungen und Betriebsunterbrechungen die wesentlichen Ursachen für finanzielle Verluste.

Die Schlagzeilen über Cyber-Angriffe auf prominente Unternehmen und Organisationen reißen nicht ab. Umfangreiche Datenschutzverletzungen und Distributed-Denial-of-Service-Angriffe (DDoS), bei der sich Kriminelle das Internet der Dinge (Internet of Things, IoT) zunutze machen, sind dabei die bekanntesten Arten solcher Attacken. Die am schnellsten wachsende Gruppe von Cyber-Verbrechen sind jedoch Cyber-Erpressung und Ransomware, wie aus dem AIG Datenreport zu Schadenfällen in der Cyber-Versicherung über einen Zeitraum von drei Jahren von 2013 bis September 2016 hervorgeht.

Erpressungen mit Verschlüsselungs-Ransomware sind demnach für 16 % der Schadenfälle während dieses Zeitraums verantwortlich. Weitere 4 % entfallen auf andere Cyber-Erpressungen. Insbesondere 2016 sind Fälle von Cyber-Erpressung rasant angestiegen. „In den ersten neun Monaten dieses Jahres verzeichneten wir zahlreiche Meldungen von Unternehmen, die Opfer von Angriffen mit Ransomware waren, wobei fast alle von ihnen auch erpresserischen Charakter hatten“, erläutert Kathy Avery, Major Loss Adjuster Financial Lines, London. „Gerade bei kleinen Unternehmen beobachten wir einen signifikanten Anstieg.“

AIG Schadenfälle im Bereich Cyber (2013 - 2016) - Nach Typ

Anmerkung: Da die Zahlen gerundet wurden, ergeben sie zusammengezählt nicht zwangsläufig 100 %.

Als Beispiel nennt sie einen Onlinehandel für Gartenutensilien. Der Besitzer stellte fest, dass Ransomware sein System infiziert und alle seine Dateien verschlüsselt hatte. Der kleine Versandhandel musste sich zwar keine Gedanken über die Gefährdung von sensiblen Daten machen, aber der Unternehmer konnte seine Kunden nicht mehr kontaktieren oder auf seine Rechnungslegung zugreifen. So entschied er sich dazu, ein Lösegeld zu zahlen, um wieder Zugriff auf seine Kunden- und Rechnungsdaten zu erhalten. Ein Forensiker von AIG unterstützte das Unternehmen im Prozess und überwachte die Entschlüsselung.

Bei Schadenfällen durch Erpressung und Denial-of-Service- (DoS) sowie DDoS-Angriffen gibt es einige Überschneidungen, da viele dieser Angriffe erpresserischen Charakter haben. Sechs Prozent der AIG gemeldeten Cyber-Schäden in den letzten drei Jahren wurden als Denial-of-Service-Angriffe eingeordnet. „Einige der DoS-Angriffe fallen in den Bereich der Erpressung", so Avery. „In vielen dieser Fälle verwenden die Angreifer eine SQL-Einschleusung mittels derer sie Daten extrahieren und anschließend mit Veröffentlichung drohen, sollte kein Lösegeld gezahlt werden."

Obwohl immer mehr Cyber-Versicherungen abgeschlossen werden und Meldungen über Cyber-Angriffe mit Erpressung zunehmen, liegt die Dunkelziffer nicht-gemeldeter Ransomware-Verluste um ein Vielfaches höher. „Lösegelder werden in der Regel in Bitcoin gezahlt. Die Leute sind manchmal überrascht darüber, wie gering einige der Lösegeldforderungen ausfallen", erläutert Avery. „Wenn man damit keine Erfahrung hat, kann es allerdings passieren, dass man sich der Gefahr eines weiteren Angriffs aussetzt, während man glaubt, seine Dateien zu entschlüsseln."

Erpressung ist in Anbetracht der Häufigkeit der Angriffe eine lukrative und relativ einfache Möglichkeit für Cyber-Kriminelle schnell an virtuelles Bargeld zu gelangen. Laut Untersuchungen der Cyber Threat Alliance haben Kriminelle in den vergangenen drei Jahren etwa 325 Millionen US-Dollar mit CryptoWalls erbeutet; eine andere Hackergruppe ist mit Hilfe der relativ simplen Ransomware CryptoLocker an über 30 Millionen US-Dollar gelangt.

McAfee Labs ordnet Ransomware ganz oben auf seiner Liste für Bedrohungen ein und erwartet sogar eine Fokussierung auf bestimmte Branchen, zu denen auch Finanzdienstleister und Kommunalverwaltungen zählen. Krankenhäuser und Arztpraxen sind ebenfalls zu einer besonderen Zielscheibe geworden. „Im Gesundheitswesen kann sich Verschlüsselungs-Ransomware sofort auf die Patientenversorgung auswirken und einen Vertrauensverlust zur Folge haben. Das macht diese Branche so verwundbar", sagt David Ferbrache, technischer Leiter bei KPMG.

„Zwischen Januar und Februar 2016 haben wir eine Veränderung und einen explosiven Anstieg unterschiedlicher Arten von Ransomware festgestellt – unterschiedliche Familien und Tools – was nahelegt, dass das Ganze zu einem „Crime-as-a-Service"-Modell geworden ist", führt er weiter aus. „Die Attacken wurden standardisiert und wir erkennen allmählich Anzeichen dafür, dass die Gruppen, die Ransomware-Angriffe durchführen, bei ihren Attacken schlauer werden."

In Fällen von Cyber-Erpressung hängt die Schwere der Schadenfälle von der Art des Unternehmens, dem Ausmaß der verursachten Betriebsunterbrechung und auch davon ab, ob eine forensische Untersuchung zur Systemwiederherstellung nötig ist. Lösegeldforderungen bleiben in der Regel gering. Bei DoS- oder DDoS-Angriffen können die Kosten, die durch das Abschalten der Webseiten entstehen, besonders hoch sein, wie das Beispiel des Online-Händlers in der Fallstudie zeigt.

„Denial-of-Service-Angriffe sind inzwischen stark standardisiert", erläutert Ferbrache. „Cyber-Kriminelle können einen DoS-Angriff für 5 oder 10 US-Dollar pro Stunde kaufen. So kann man eine öffentliche Webseite angreifen, indem zu viel Datenverkehr künstlich erzeugt wird, um die Webseite damit zum Erliegen zu bringen."

„Zurzeit macht sich jeder Sorgen über großangelegte DDoS-Angriffe", erläutert er weiter. „Wir haben es jetzt mit Botnets im Internet der Dinge zu tun, wo digitale Videorekorder, CCTV-Kameras und Heimrouter zu Angreifern werden. Dies führt zu störendem Datenverkehr in extrem hohen Ausmaßen."

Kriminelle Akteure haben in den vergangenen drei Jahren etwa 325 Millionen US-Dollar durch CryptoWall Programme erbeutet

Im Oktober 2016 wurden die Server des DNS-Anbieters Dyn Opfer eines massiven DDoS-Angriffs, der eine weitflächige Störung verursachte. An dem DDoS-Angriff war ein Botnet beteiligt, das über viele Millionen angeschlossener Geräte gesteuert wurde. Hierzu zählten Überwachungskameras, Webcams, intelligente Thermostate und sogar Baby-Monitore, die mit der Schadsoftware Mirai infiziert waren. Attacken dieser Größenordnung nehmen immer weiter zu. Laut neuestem Sicherheitsbericht „State of the Internet" von Akamai sind diese gegenüber dem Vorjahr um bis zu 138 % gestiegen.

Für die Opfer von Ransomware oder Denial-of-Service-Angriffen sind die Kosten für Betriebsunterbrechungen um ein Vielfaches höher als der eigentliche Schaden. Die Hälfte der Befragten erläuterte in einer kürzlich durchgeführten Umfrage, dass der finanzielle Verlust teilweise bis zu 100.000 US Dollar pro Stunde betragen kann. „Ich kenne einen Fall, bei dem die Lösegeldforderung 262 britische Pfund betrug und die Forderung des Kunden gegenüber seiner Versicherung aufgrund der Geschäftsunterbrechung siebenstellig war", so Stephen Tester, Partner bei CMS Cameron McKenna. „Dabei wurde die Webseite des Unternehmens über das Wochenende aus dem Netz genommen."

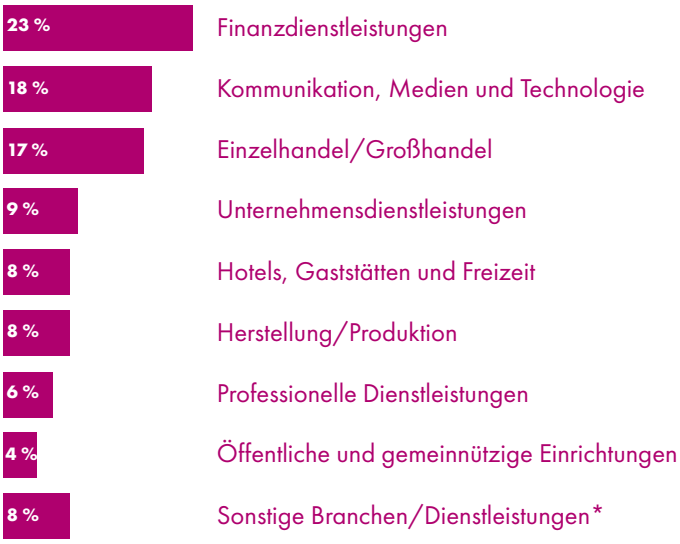
Während zurzeit nur vier Prozent der AIG Cyber-Schadenfälle in Europa mit Betriebsunterbrechungen einhergehen (und weitere vier Prozent der Schadenfälle auf Systemausfall/-unterbrechung entfallen), erwartet der Versicherer, dass Cyber-Schadenfälle mit Betriebsunterbrechungen in Zukunft häufiger vorkommen und gravierender ausfallen. Eine schnelle Reaktion auf Datenschutzverletzungen kann potenzielle Auswirkungen abschwächen.

Gesetze zum Datenschutz werden in Zukunft immer wichtiger werden

Bei AIG gemeldete Schäden aufgrund von Datenschutzverletzungen fallen unter zwei getrennte Forderungskategorien: die von Hackern verursachten Schäden sowie Schäden, die durch Nachlässigkeit eines Mitarbeiters entstanden sind. Zusammen ergeben sie mehr als ein Fünftel der Schadenfälle in der Cyber-Versicherung (22 %), die in den vergangen drei Jahren eingingen (siehe S. 2). Die steigenden Kosten von Datenschutzverletzungen, damit zusammenhängende Auswirkungen auf die Reputation und zunehmende Meldepflichten werden zukünftig wahrscheinlich sowohl die Häufigkeit als auch die Schwere solcher Schadenfälle beeinflussen.

Da ist es nicht überraschend, dass die Mehrzahl der Schadenfälle in der Cyber-Versicherung derzeit auf Branchen entfällt, die ihre Kunden informieren müssen, wenn sensible Daten gefährdet waren. Finanzdienstleistungen führen mit beinahe einem Viertel aller Cyber-Schäden, die AIG in den vergangenen drei Jahren gemeldet wurden die Liste an, gefolgt von Kommunikation, Medien und Technologie einschließlich Telekommunikation (18 %).

AIG Schadenfälle in der Cyber-Versicherung (2013 - 2016) - Nach Branche



* Bau, Essen und Trinken, Informationsdienstleistungen, sonstige Dienstleistungen, Transport, Landwirtschaft und Fischerei, Energie und Immobilien

Anmerkung: Da die Zahlen gerundet wurden, ergeben sie zusammengezählt nicht zwangsläufig 100 %.

Die Datenschutz-Grundverordnung (DSGVO), welche ab Mai 2018 anwendbar ist, schreibt Unternehmen, die ihren Sitz in der EU haben, und Unternehmen, die sich außerhalb der EU befinden und Daten von EU-Bürgern verarbeiten vor, dass sie eine Datenschutzverletzung innerhalb von 72 Stunden nach Auftreten melden – vorausgesetzt das ist möglich. Unternehmen, die es versäumen, ihre Daten angemessen zu schützen, müssen mit erheblichen Geldstrafen rechnen. Ein Unternehmen kann mit einer Geldstrafe von bis zu zwei Prozent seines jährlich erzielten weltweiten Umsatzes belegt werden, wenn Aufzeichnungen nicht in Ordnung sind, die Aufsichtsbehörden nicht sachgemäß über Datenschutzverletzungen informiert wurden oder keine Folgenabschätzungen durchgeführt wurden. Schwerwiegendere Verstöße können auch eine Geldstrafe von vier Prozent rechtfertigen.

AIG Schadenfälle in der Cyber-Versicherung (2013 - 2016) - Anzahl

Die neuen Datenschutzregelungen und Medienberichte über Datenschutzverletzungen werden die Nachfrage nach Cyber-Versicherungen voraussichtlich weiter ansteigen lassen. In der Folge wird dies zu einem weiteren Anstieg der Schadenfälle in der Cyber-Versicherung führen. José Martínez, VP Financial Lines Großschadenforderungen, London, erläutert, dass die jährlichen Schäden von AIG in Europa im Rahmen von eigenständigen Cyber-Policen von nur zwei im Jahr 2013 auf 121 bis September 2016 angestiegen sind. Die Gesamtjahresprognose für 2016 beläuft sich sogar auf 170 Schäden.

Die durchschnittlichen Gesamtkosten einer Datenschutzverletzung betragen nach einer Studie von Ponemon und IBM inzwischen 4 Millionen US-Dollar weltweit und sind seit 2013 somit um 29 % gestiegen. Trotzdem kann die Schwere einiger Schadenfälle, laut Avery, durch schnelles und professionelles Handeln abgemildert werden. „Aufgrund unseres Vorgehens bei der Schadenbearbeitung können die meisten Vorfälle innerhalb der ersten 48 Stunden unter Kontrolle gebracht werden."

„Bei den europäischen Datenschutzverordnungen, die jetzt hinzukommen, ist es natürlich so, dass die Geldstrafen niedriger sein sollten, wenn man nachweisen kann, dass man bei einer Datenschutzverletzung richtig gehandelt hat und mit guten Systemen ausgerüstet war", fügt Kathy Avery hinzu.

Die durchschnittlichen Gesamtkosten einer Datenschutzverletzung betragen inzwischen 4 Millionen US-Dollar weltweit und sind seit 2013 somit um 29 % gestiegen

Bei Schadenfällen in der Cyber-Versicherung gibt es in den meisten Fällen ein menschliches Element. Das kann die Nachlässigkeit eines Mitarbeiters sein oder das vorsätzliche Handeln eines aktuellen oder früheren Mitarbeiters, der beispielsweise seinem Ärger Luft machen will. Das Risiko, dass Mitarbeiter sich zu Phishing-Betrügereien verleiten lassen oder falsche Daten versenden, kann durch Schulungen und das Implementieren geeigneter Kontrollen und Systeme verringert werden. Bei sechs Prozent der Cyber-Schäden, die bei AIG in Europa zwischen 2013 und 2016 gemeldet wurden, war der Verlust oder Diebstahl von Notebooks, Datensticks oder Festplatten die Ursache.

Menschliches Versagen und/oder Insiderwissen sind zudem eine häufige Schwachstelle, die sich der sogenannte „Friday afternoon fraud" („Freitagsnachmittagsbetrug") zunutze macht. Ziel sind insbesondere Anwaltskanzleien, die häufig an einem Freitagnachmittag angegriffen werden, weil es dann unwahrscheinlich ist, dass der Betrug vor dem darauffolgenden Montag entdeckt wird. Kriminelle werden immer geschickter darin, Firmen von der Herausgabe sensibler Daten zu überzeugen. So verwenden sie beispielsweise Daten von echten Transaktionen, um als legitimer Ansprechpartner wahrgenommen zu werden.

In der Regel werden bei Betrügereien dieser Art reguläre E-Mails verwendet, was für Versicherungen die Frage aufwirft, ob es sich bei dieser Art von Vorfällen um Cyber-Schäden oder um die Kategorie Vertrauensschaden handelt, insbesondere wenn in einer gefälschten E-Mail eine ähnliche aber nicht identische E-Mail-Adresse verwendet wird. „Wir haben einige Schadenfälle im Blick, bei denen die Deckung grenzwertig ist", sagt Kathy Avery. „In vielen Fällen handelt es sich um herkömmlichen Betrug, der elektronisch begangen wird, der aber nicht mit einer tatsächlichen Sicherheitsverletzung einhergeht."

Die sogenannte „Fake president fraud" (die „Chef-Masche" oder der „Geschäftsführer-Trick") ist ein weiterer beliebter Trick der Betrüger. Dabei wird in der Regel ein Mitarbeiter aus der Buchhaltung telefonisch oder per E-Mail kontaktiert. Der Anrufer gibt vor, ein leitender Angestellter zu sein und weist den Mitarbeiter an, eine dringende Zahlung zu tätigen. Verluste aus „business email compromise" (kompromittierte Geschäfts-E-Mails), wie sie in den USA genannt werden, sind Angaben des Crime Complaint Center des FBI zufolge, seit Mai 2016, auf 3,1 Milliarden US-Dollar gestiegen: Eine signifikante Steigerung um 1.300 %.

„Das ist nur die Spitze des Eisbergs, denn dem FBI werden ausschließlich Fälle gemeldet, die in den USA oder auf internationaler Ebene aufgetreten sind", gibt Ferbrache von KPMG zu bedenken. „Business email compromise ist ein riesiges Problem. Manchmal sind bei diesen Betrügereien zunächst Anwalts- oder Steuerberaterkanzleien das Ziel. Die Adressen dieser Kanzleien dienen den Kriminellen dann als Vehikel, die zum Versand der E-Mails verwendet werden, die das Zielunternehmen täuschen und dort vertrauliche Daten „abfischen" sollen.

„Mit dem "Fake-President"-Betrug werden zurzeit durchschnittlich 160.000 US-Dollar erbeutet", fügt er hinzu. „Der größte Betrug, der unserem Wissen nach in Europa gemeldet wurde, lag bei 40 Millionen Euro. Ich weiß jedoch nicht, ob es sich hierbei um ein Cyber-Verbrechen oder nur um wirklich gut organisierten Trickbetrug gehandelt hat."

Fallstudien zu Cyber-Schäden

Die folgenden Fälle sind Beispiele, die in den letzten Jahren AIG gemeldet wurden. Diese zeigen die große Bandbreite an Schäden, die unser Versicherungsprodukt CyberEdge® abdeckt. Sie verdeutlichen auch, dass Cyber-Schäden jedes Unternehmen - von KMUs (kleine- und mittelständische Unternehmen) bis hin zum Großunternehmen - treffen können.

Ransomware-Angriff auf eine Online-Stickerei

Kurz vor Weihnachten 2015 wurde eine Online-Stickerei in Großbritannien Opfer einer Ransomware-Attacke. Der Angreifer erstellte zwei Benutzerkonten und versuchte Kundendaten sowie Informationen zu Bestellungen, Lagerbeständen und Konten zu entschlüsseln und zu entfernen. Er hinterließ zudem eine Lösegeldforderung, in der er den Versicherungsnehmer anwies, eine bestimmte E-Mail-Adresse zu kontaktieren.

Während es dem Angreifer nicht gelang, die Daten zu entschlüsseln, konnte er dennoch zahlreiche Dateien erfolgreich löschen sowie Daten hin und her bewegen. Da Daten an einen anderen Ort verschoben wurden, konnte sich der Versicherungsnehmer nicht auf ihre Genauigkeit verlassen und war außer Stande, seine Geschäftstätigkeit über das System weiterhin abzuwickeln. Die letzte Datensicherung wurde vier Tage vor dem Angriff durchgeführt, sodass Daten der laufenden Woche ebenfalls verloren gingen.

AIG vermittelte dem Versicherungsnehmer zunächst sowohl eine rechtliche als auch eine IT-Beratung. Nachdem ersichtlich wurde, dass Daten von Dritten während des Angriffs nicht gefährdet waren, wurde der Versicherungsnehmer darauf hingewiesen, dass eine Mitteilung an die Datenschutzbehörden nicht notwendig sei.

Die IT-Berater des Versicherungsnehmers gaben zudem wertvolle Hinweise, wie die Auswirkungen der Sicherheitsverletzung abgemildert werden können und welche Vorkehrungen zu treffen sind, um die Wahrscheinlichkeit eines weiteren Vorfalls zu mindern. Der Versicherungsnehmer wurde insbesondere drauf hingewiesen, die Daten des betroffenen Servers zu sichern, um zu untersuchen wie es zu der Sicherheitsverletzung kommen konnte, sowie seinen Notfallplan zu überprüfen.

Verschlüsselung von Dateien auf internen Netzlaufwerken von Versicherungsvermittlern

Einer der Computer des Versicherungsnehmers war mit der Schadsoftware CryptoWall infiziert, die bestimmte, auf dem Computer gespeicherte Dateien sowie das interne Netzlaufwerk des Versicherungsnehmers verschlüsselt hat. Die Namen der Dateien wurden in „help_your_files.png“ geändert, und es wurde ein Lösegeld gefordert, um wieder auf die Dateien zugreifen zu können.

Der Versicherungsnehmer mit Sitz in Großbritannien vermutete, dass in den verschlüsselten Dateien Kundendaten wie Namen und Adressen gespeichert seien, sie jedoch, keine weiteren persönlichen Daten oder Finanzinformationen enthalten würden. Es gab keine Anzeichen dafür, dass auf Daten in den verschlüsselten Dateien zugegriffen wurde, diese exportiert wurden oder dass es aufgrund von routinemäßigen Backups des IT-Systems des Versicherten zu einem Datenverlust gekommen wäre.

Der Versicherungsnehmer erhielt rechtliche Beratung im Hinblick auf das Ausmaß seiner Meldepflichten an die britische Finanzaufsichtsbehörde (FCA). Externe IT-Berater rieten dem Versicherten darüber hinaus, sofortige Maßnahmen zur Eindämmung des Vorfalls einzuleiten (wie beispielsweise das Teilen von Dateien zwischen Nutzern einzuschränken), und schlugen vor, weitere Maßnahmen zu ergreifen, um das Auftreten solcher Vorfälle in Zukunft zu vermeiden.

Distributed-Denial-of-Service-Angriff (DDoS) auf einen Online-Händler

Die Webseite des Versicherten war nach einem DDoS-Angriff für Kunden nicht mehr zugänglich. Vor dem Angriff erhielt der Versicherungsnehmer eine E-Mail mit der Nachricht, dass der Schutz seiner Webseite extrem schwach sei und sie deswegen offline gesetzt würde, bis eine Zahlung von 3.000 britischen Pfund erfolgte. Während des Angriffs gingen weitere Lösegeldforderungen in Höhe von 500 britischen Pfund ein.

Der Versicherungsnehmer erlitt aller Wahrscheinlichkeit nach Verkaufseinbußen, weil seine Webseite nicht erreichbar war. Das genaue Ausmaß des Verlusts ließ sich allerdings nicht bemessen. Der Versicherungsnehmer glaubte nicht, dass auf Daten zugegriffen wurde oder Daten extrahiert wurden. Ihm wurde mitgeteilt, dass aufgrund des Angriffs keine rechtlichen Meldepflichten bestünden.

Es traten jedoch verschiedene IT- und Reputationsprobleme auf, die ein weiteres Vorgehen erforderlich machten. Der Versicherte wurde darauf hingewiesen, dass neben externen IT-Beratern auch PR-Berater zu seiner Verfügung stehen, die ihm beim Umgang mit den Auswirkungen der vorübergehenden Nichterreichbarkeit seiner Webseite helfen könnten.

Mailing eines Inkassounternehmens

Der Versicherungsnehmer machte aufgrund eines Fehlers mit der Software-Plattform eines Drittanbieters die Erfahrung eines unberechtigten Mailings an seine Kunden. Ein Dritter forderte 11.275 britische Pfund von ihm für Arbeiten, die infolge dieses Mailings durchgeführt wurden. Der Versicherte versuchte sich diese Summe vom Betreiber der Plattform zurückzuholen, es bestand dennoch das Risiko, dass er den Betrag würde zahlen müssen.

Aus diesem Vorfall ergab sich eine Reihe von Problemen. Der Versicherungsnehmer erhielt rechtliche Beratung hinsichtlich des Umfangs seines Vertrags mit dem Betreiber der Plattform und hinsichtlich der Möglichkeit, die geforderte Summe vom Betreiber zurückzuverlangen. Darüber hinaus wurde der Versicherte zum Thema Datenschutz beraten, obwohl es infolge des Vorfalls anscheinend nicht zum Verlust, zur Freigabe, zur Gefährdung oder zur Verfälschung von persönlichen Daten gekommen war.

Bei der Beweissicherung wurde der Versicherte von externen IT-Beratern unterstützt, die beim Nachweis halfen, dass der Vorfall nicht durch einen Fehler im System des Versicherten oder durch einen Mitarbeiter des Versicherten verursacht worden war. Da von zahlreichen Empfängern des Mailings Beschwerdebriefe eingingen, wurde dem Versicherten zudem geraten, sich an eine PR-Agentur zu wenden, die ihn zu entsprechenden PR-Maßnahmen beraten sollte.

Cryptolocker Attacke auf eine Bank

Freitagabend um kurz vor 20 Uhr wurde eine Bank in Irland mit Cryptolocker-Malware angegriffen. Durch die Malware wurden verschiedene Laptops und Computer der Bank infiziert und verschlüsselt. Den Angreifern gelang es auch einen Server mit ca. 11.000 Kundendaten, darunter Kauf- und Verkaufsaufträge, Aktiendepots und Konten zu verschlüsseln.

Das vorhandene Anti-Virus-Programm der Bank konnte die Infizierung der Systeme nicht verhindern. In kurzer Zeit war die Bank jedoch in der Lage alle betroffenen Systeme zu erfassen und vom Netzwerk zu trennen. Die Daten auf dem Server konnten über ein Back-Up wiederhergestellt werden.

Nach Anruf der AIG Cyber-Hotline, erhielt die versicherte Bank IT- und rechtliche Unterstützung. Da weder vertrauliche noch Daten öffentlich zugänglich waren, konnte die Bank auf eine Benachrichtigung der Behörden verzichten.

Von einem IT-Consultant erhielt die Versicherungsnehmerin weitere Unterstützung bei der Aufarbeitung des Angriffes sowie Hinweise wie in Zukunft etwaige Angriffe verhindert werden können.

Kundendaten im DarkNet

Im Winter 2016 wurde der CISO eines Finanzdienstleisters informiert, dass vertrauliche Kundendaten seines Instituts im DarkNet zum Kauf angeboten werden. Mit der Unterstützung von IT-Forensikern konnte das gesamte Ausmaß sowie die Echtheit der Daten verifiziert werden. Die durch AIG vermittelten IT-Forensiker konnten auch den Ursprung der Daten nachverfolgen: Es stellte sich heraus, dass wenige Wochen vor der Veröffentlichung im DarkNet Daten durch eine SQL-Attacke entwendet werden konnten.

Über 60.000 Datensätze, darunter vertrauliche Kundendaten sowie Kontoinformationen, wurden gestohlen. Der Finanzdienstleiter informierte daraufhin die entsprechenden Behörden und die Börse. Ebenfalls wurden die betroffenen Kunden informiert. Diese Schritte wurden zusammen mit PR-Experten und Rechtsanwälten durchgeführt, die durch AIG vermittelt wurden.

Für die weitere Kommunikation mit Kunden und den Medien konnte die Versicherungsnehmerin auf Unterstützung von PR Beratern zugreifen. Um einen möglichen Missbrauch mit den veröffentlichten Daten zu vermeiden, wurden diverse Überwachungssysteme eingerichtet.

Durch die Unterstützung von externen Rechtsanwälten, IT-Spezialisten und PR-Beratern war die Versicherungsnehmerin in der Lage professionell auf den Vorfall zu reagieren. Durch die zusätzlich zur Verfügung stehenden externen Ressourcen konnte das Ausmaß des Vorfalls begrenzt, und zukünftige Schadenfälle vermieden werden.

Wichtige Fragen an einen Cyber-Versicherer:

1. *Hat der Versicherer Erfahrung beim Umgang und bei der Bearbeitung von Schadenfällen?*
2. *Sucht der Versicherer kontinuierlich nach neuen Wegen, um Versicherte vor möglichen Cyber-Risiken zu schützen?*
3. *Bietet der Versicherer beständigen Schutz auf der ganzen Welt, mit lokalen Policen und lokalen Ansprechpartnern?*
4. *Hat der Versicherer bereits Kontakte zu erstklassigen forensischen Experten aus den Bereichen IT, Recht und PR?*
5. *Verfolgt der Versicherer im Hinblick auf das Underwriting und die Schadenbearbeitung einen ganzheitlichen Ansatz und schwächt das Risiko eines Schadens bereits im Vorfeld ab, indem er entsprechende Dienstleistungen und Datenschutzexperten präventiv anbietet?*
6. *Hat der Versicherer einen externen Berater, der die Bearbeitung von Schadenfällen übernimmt, oder verfügt er über ein internes Team von spezialisierten Schadenregulierern, das einen fortlaufenden Dialog zwischen Schadenbearbeitung und Underwriting ermöglicht?*

Über die Autoren

Kathy Avery leitet im Bereich Financial Lines die Großschadenregulierung bei AIG Europe Limited. Sie ist auf Berufshaftpflicht- und Cyber-Schäden in Großbritannien und auf internationaler Ebene spezialisiert. José Martínez ist VP Financial Lines im Bereich Großschadenregulierung bei AIG in EMEA.

Vorgehensweise

Im Oktober 2016 führte AIG Europe eine Analyse von 221 Schadenfällen durch, die von 2013 bis September 2016 im Rahmen von Cyber-Policen gemeldet wurden.

Kontakt

AIG verfügt über Experten auf den Gebieten Cyber-Schäden und Underwriting in ganz Europa. Unser erfahrenes Team befasst sich jedes Jahr mit einem breiten Spektrum an Cyber-Schäden. Für weitere Informationen wenden Sie sich bitte an einen Ansprechpartner in Ihrer Region:

Nepomuk Loesti

Head of Liability and Financial Lines
Deutschland/Österreich/Schweiz
Financial Lines | AIG Property Casualty
AIG Europe Limited, Direktion für Deutschland
Speicherstraße 55, 60327 Frankfurt
T +49 (0)69 97113-271
nepomuk.loesti@aig.com

Alexander N. Shopov

Direktor Vertrieb Österreich Distribution
AIG Property Casualty
AIG Europe Limited, Branch Austria
Herrengasse 1-3 | 1010 Wien
T +43 (0)1 5332500-38
alexander.shopov@aig.com

Elisabeth André-Raecke

Senior Underwriter
Practice Leader Financial Institutions Switzerland
Financial Lines | AIG Property Casualty
AIG Europe Limited | Avenue Louis-Casaï 18 | 1211 Genf, Schweiz
T +41 (0)22 747 75 75
elisabeth.andre@aig.com

Giv Kahrom

Underwriter
Commercial Institutions & Cyber Risks
Financial Lines | AIG Property Casualty
AIG Europe Limited | Sägereistrasse 29 | CH-8152 Glattbrugg, Schweiz
T +41 43 333 37 35
giv.kahrom@aig.com

www.aig.com

01/17 DEL00001530