Martin Zschech

Schlüsselrisiken für den Finanzdienstleistungssektor

Manchmal reicht ein einzelner Mann, um eine ganze Bank zum Untergang zu bringen: In den 90er Jahren des vergangenen Jahrhunderts hatte der legendäre Derivatehändler Nick Leeson Lücken in den internen Kontrollsystemen der traditionsreichen Barings Bank genutzt und versucht, seine immensen Verluste durch immer waghalsigere Spekulationen zu kompensieren. 1995 kippte die bis dahin schon sehr fragile Balance seiner geschäftlichen Aktivitäten. Vier Wochen lang versuchte Leeson noch sein einbrechendes Kartenhaus aus Terminkontrakten und ähnlichen Finanzinstrumenten zu stabilisieren, doch das gelang ihm nicht mehr.

Immer höher stiegen die Verluste, die auf Rechnung der Barings Bank gingen, in deren Namen er stets gehandelt hatte. Am 23. Februar 1995 zog Leeson schließlich die Reißleine und setzte sich mit seiner Frau nach Kuala Lumpur ab. Er wurde später am Frankfurter Flughafen gefasst und zu sechseinhalb Jahren Haft verurteilt. Die Barings Bank, die vor Leeson immerhin mehr als zwei Jahrhunderte stürmischer Geschichte überstanden und unter anderem den Kauf Louisianas durch die Vereinigten Staaten von Amerika finanziert hatte, wurde liquidiert. Lediglich der Name blieb bestehen.

Enorme Komplexität

Der „Leeson-Fall" mag ein Extrembeispiel sein – und kriminelles Fehlverhalten von Mitarbeitern die Ausnahme. Doch auch wenn die Branche ihr Risikomanagement nach der Finanzkrise vor einigen Jahren deutlich verbessert hat, haben Finanzinstitute mehr denn je Mühe, effektiv mit den vielfältigen Risiken umzugehen, die sich aus ihren Geschäftsaktivitäten ergeben. Denn die Risiken, die heutzutage auf den Finanzdienstleistungssektor einwirken, sind komplexer als ein einzelner korrupter Mitarbeiter.

Die Allianz Global Corporate & Specialty (AGCS) ist als Industrieversicherer der Allianz Gruppe einer der Partner beim Risikomanagement von Banken, Vermögensverwaltern, Private-Equity-Fonds und anderen Akteuren im Finanzdienstleistungssektor weltweit und hat für ihren neusten Report eine Vielzahl von Gefährdungen identifiziert, auf die sich die Organisationen in einer zunehmend unsicheren Finanz- und Wirtschaftswelt vorbereiten müssen – von Cybergefahren bis hin zu Compliance und ESG-Anforderungen. Zudem wurden Schadentrends anhand von 7654 Versicherungsschäden aus den Jahren 2015 bis 2021 für Finanzinstitute analysiert.

> „Es gibt eine Vielzahl von Gefährdungen in einer zunehmend unsicheren Finanz- und Wirtschaftswelt."

Wenn es nach Cyber-Security-Experten geht, dann müssen sich Finanzinstitute auf einem „perfekten Sturm" von Cyberkriminalität vorbereiten. Die Covid-19-Pandemie hat zu einem schnellen und weitgehend ungeplanten Anstieg der Arbeit von zu Hause und des elektronischen Handels sowie einer rasanten Beschleunigung der Digitalisierung geführt. Dieses Umfeld bietet ein perfektes Umfeld für Kriminelle. Trotz erheblicher Ausgaben für Cybersicherheit sind sie wegen der proprietären Kunden- und Transaktionsdaten mehr denn je ein attraktives Ziel und sehen sich mit einer Vielzahl von Cyberbedrohungen konfrontiert. Der Solarwinds-Angriff auf Banken und Aufsichtsbehörden und die Carbanak- und Cobalt-Malware-Kampagnen auf über 100 Finanzinstitute sind nur drei Beispiele von vielen.

Cyberangriffe

Ganz oben auf der Bedrohungsagenda der Cyberexperten in den Finanzinstituten stehen Ransomware-Angriffe, die in Häufigkeit und Schwere weiter zunehmen und bei denen immer höhere Lösegeldforderungen gestellt werden. Im vergangenen Jahr warnte zudem die US-Börsenaufsichtsbehörde Securities Exchange Commission vor einem Anstieg der Anzahl und Raffinesse von Ransomware-Angriffen auf US-Finanzinstitute.

Laut VMware haben sich die Ransomware-Angriffe zwischen Februar und Ende April 2020 verneunfacht. Unter anderem wurde der US-Kreditgeber Flagstar Bank Anfang 2020 Opfer einer Ransomware-Attacke, bei der Hacker persönliche Daten online veröffentlichten, um Geld zu erpressen. Vergangenes Jahr schloss die chilenische Bank Banco Estado ihre Filialen nach einem Ransomware-Angriff. Im März 2021 war auch CNA Hardy von

einer ausgeklügelten Ransomware-Attacke betroffen, die sich auf die Betriebsabläufe und E-Mail-Systeme auswirkte und den Versicherer mehrere Wochen lang erheblich beeinträchtigte.

Da viele Mitarbeiter von zu Hause arbeiten und unter erhöhtem Stress stehen, hat Covid-19 Möglichkeiten für Cyberkriminelle geschaffen, verschiedene Betrügereien und Cyberangriffe durchzuführen. Das US Federal Bureau of Investigation (FBI) erhielt allein im Jahr 2020 über 28 500 Meldungen im Zusammenhang mit Covid-19-Cyberkriminalität. Bei vielen Vorfällen ging es darum, Fördergelder und Darlehen des Paycheck Protection Program (PPP) auszunutzen sowie Covid-19-bezogene Phishing-Angriffe zu nutzen, um Geld oder persönliche Daten zu stehlen.

Business-Email-Compromise-(BEC)-Angriffe, auch bekannt als „Fake President", sind ein weiteres Problem für Finanzinstitute, die im Auftrag ihrer Kunden eine große Anzahl von Zahlungen mit hohem Wert durchführen. Die Kosten von BEC-Angriffen erreichten im Jahr 2020 1,86 Milliarden US-Dollar und machten damit fast die Hälfte aller gemeldeten Verluste durch Cyberkriminalität aus. Solche Angriffe werden immer raffinierter und beinhalten zunehmend Identitätsdiebstahl und die Umwandlung von Geldern in Kryptowährungen.

Auch Geldautomaten- oder „Jackpotting"-Angriffe stellen weiterhin eine Bedrohung dar. Am 13. Juli 2020 schaltete die belgische Sparkasse Argenta 143 Geldautomaten ab, nachdem Kriminelle versucht hatten, über ihre Netzwerkserver die Kontrolle über ihre Geldautomaten zu übernehmen. Diese Angriffe sind immer raffinierter geworden und in den vergangenen fünf Jahren hat „Jackpotting" den Finanzdienstleistungssektor Millionen Euro gekostet.

Eine der größten und raffiniertesten Cyberattacken des vergangenen Jahres, der Solar-Winds-Vorfall, war ein Angriff auf die Lieferkette. Hacker verschafften sich Zugang zum Netzwerk von Solar Winds und injizierten Malware in die Management-Software, um Tausende von Organisationen, darunter Banken und Behörden, anzugreifen. Der Vorfall bei Solar Winds – und jüngst die Kaseya-Attacke – führen deutlich vor Augen, wie anfällig der Finanzdienstleistungssektor für Cyberangriffe und Systemausfälle ist, weil er von Drittanbietern und Dienstleistern abhängig ist.

Auch die immer weiter verbreiteten Cloud-basierten Services sind mit Blick auf Cyber ein zweischneidiges Schwert. Die meisten Finanzinstitute nutzen inzwischen Software, die von Cloud-Diensten betrieben wird, um auf zusätzliche Verarbeitungskapazitäten zuzugreifen, aber auch für die IT-Infrastruktur oder zur Durchführung bestimmter Prozesse, wie zum Beispiel Betrugserkennung oder Analysen.

Auf der einen Seite entwickeln Cloud-Anbieter Tools, die Unternehmen dabei helfen, ihre Cyberrisiken zu managen und zu mindern, doch die wachsende Abhängigkeit von einer relativ kleinen Anzahl von Cloud-Anbietern und einer komplexen Cloud-Infrastruktur schafft potenziell große und systemische Risiken. Eine Umfrage der Bank of England unter Banken und Versicherern im vergangenen Jahr ergab, dass die Bereitstellung von IT-Infrastruktur in der Cloud bereits stark konzentriert ist – die beiden größten Infrastructure-as-a-Service-Anbieter hatten bei Banken einen Marktanteil von etwa zwei Dritteln.

Compliance-Herausforderungen

Wie Finanzinstitute mit den Risiken der Cloud umgehen, wird in Zukunft entscheidend sein. Denn zusätzlich zu den immer raffinierten Angriffsmustern der Hacker-Industrie ist gegenwärtig ein Paradigmenwechsel in der regulatorischen Sicht auf Datenschutz und Cybersicherheit zu beobachten. Während die Aufsichtsbehörden früher darauf bedacht waren, Anreize für Unternehmen zu schaffen, in Cybersicherheit zu investieren, fokussieren sie sich jetzt immer stärker auf Verbraucherrechte und Datenschutz.

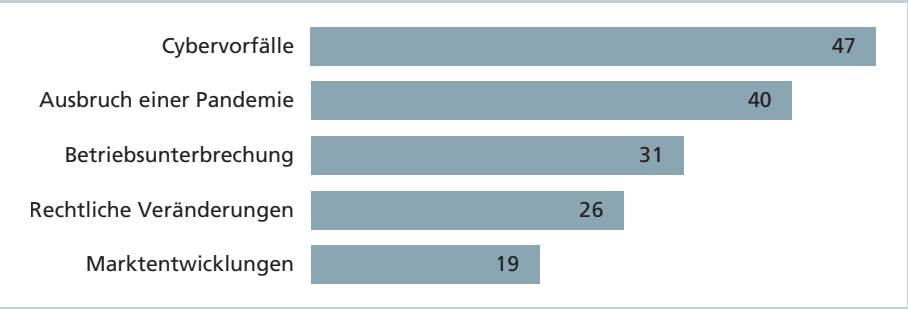
Mit der Datenschutzgrundverordnung in Europa und dem California Consumer Privacy Act in den USA müssen Banken und Finanzdienstleister Datenschutzvorschriften und die Vorgaben der Aufsichtsbehörden korrekt umsetzen – und nicht nur auf die IT-Sicherheit achten. Nach einer Reihe größerer Ausfälle bei Banken und Zahlungsdienstleistern konzentrieren sich die Aufsichtsbehörden zunehmend auf die Themen Geschäftskontinuität, robuste Prozesse und das Management von Risiken durch Drittanbieter. Notfallpläne und Krisenmanagementprozesse, die ebenfalls getestet werden müssen,

Martin Zschech

Regional Head of Distribution, verantwortlich für den Vertrieb in Zentral- und Osteuropa, Allianz Global Corporate & Specialty (AGCS), München

Banken, Vermögensverwalter, Private-Equity-Fonds, Versicherer und andere Akteure im Finanzdienstleistungssektor stehen vor einer Zeit erhöhter Risiken. Neben bewusstem und unbewusstem menschlichen Fehlverhalten rücken Gefahren aus dem Cyber-Space, eine wachsende Belastung durch Compliance, ESG-Anforderungen und die Auswirkungen der Covid-19-Pandemie zunehmend in den Blickpunkt der Risikomanager in Finanzinstituten. Der Autor beschreibt mögliche Entstehungsgeschichten der Risiken und ihre Folgen für Finanzdienstleister. Um der zunehmenden Komplexität nicht schutzlos ausgeliefert zu sein, plädiert er für eine sehr viel breitere Aufstellung des Risikomanagements sowie einen engen Austausch zwischen den Versicherten und spezialisierten Teams aus der Assekuranz. (Red.)

Top-5-Risiken im Bereich Finanzdienstleistungssektor (in Prozent)



Die 10. jährliche Umfrage des Allianz Risk Barometers wurde unter Allianz Kunden (globale Unternehmen), Maklern und Branchenverbänden durchgeführt. Außerdem wurden Risikoberater, Underwriter, leitende Angestellte und Schadenexperten im Unternehmensversicherungssegment von Allianz Global Corporate & Specialty und andere Allianz Einheiten befragt. Anzahl der Befragten: 931. Die Zahlen geben als Prozentsatz an, wie oft ein Risiko ausgewählt wurde. Die Zahlen addieren sich nicht zu 100 Prozent, da bis zu drei Risiken ausgewählt werden konnten.
Quelle: Allianz Global Corporate & Specialty SE

sind daher für alle Finanzinstitute ein Muss.

Verstöße gegen Datenschutz

Die Folgen von Datenschutzverletzungen sind weitreichend, mit einer aggressiveren Durchsetzung, höheren Bußgeldern und regulatorischen Kosten sowie einer wachsenden Haftung gegenüber Dritten. Durch die Datenschutzgrundverordnung sind die Anzahl und die Höhe von Bußgeldern bei Datenlecks in der EU gestiegen, während Jurisdiktionen auf der ganzen Welt strengere Datengesetze eingeführt haben. Auf Datenschutzverstöße und behördliche Maßnahmen folgen zunehmend Rechtsstreitigkeiten, wobei eine Reihe von Sammelklagen sowohl in Großbritannien als auch in den USA anhängig sind. Eine Datenpanne bei der Bank Capital One im Jahr 2019 führte zu einer Geldstrafe in Höhe von 80 Millionen US-Dollar und einer Reihe von Klagen betroffener Kunden.

Die Anwendung neuer Technologien wie Künstliche Intelligenz (KI), Biometrie und virtuelle Währungen wird in Zukunft wahrscheinlich neue Risiken und Haftungsfragen mit sich bringen, zum großen Teil auch bezüglich Compliance und Regulierung. Bei KI gab es in den USA bereits regulatorische Ermittlungen im Zusammenhang mit der Verwendung von unbewussten Verzerrungen in Algorithmen zur Kreditwürdigkeitsprüfung.

Außerdem gab es eine Reihe von Gerichtsverfahren im Zusammenhang mit der Erfassung und Nutzung biometrischer Daten. Die wachsende Akzeptanz von Digital- oder Kryptowährungen als Anlageklasse wird eine Reihe operativer und regulatorischer Risiken für Finanzinstitute mit sich bringen. Darunter fallen Unsicherheiten in Bezug auf potenzielle Vermögensblasen und Bedenken hinsichtlich Geldwäsche, Ransomware-Angriffen, Haftungsforderungen Dritter und sogar ESG-Themen, da das „Mining" oder die Schaffung von Kryptowährungen große Mengen an Energie verbraucht. Die Zunahme von Börseninvestitionen, die durch soziale Medien beeinflusst werden, könnte das Risiko von Verkaufsfehlern erhöhen – bereits heute eine der Hauptursachen für Versicherungsansprüche.

Klimawandel

Finanzinstitute und Kapitalmärkte gelten als wichtige Akteure, um den Klimawandel zu bekämpfen und Nachhaltigkeit zu fördern. Auch hier gibt die Regulierung das Tempo vor. Seit 2018 wurden weltweit mehr als 170 ESG-Regulierungsmaßnahmen eingeführt – vor allem in Europa. Die Regulierungsflut in Kombination mit uneinheitlichen Ansätzen in verschiedenen Ländern und mangelnder Datenverfügbarkeit stellt Finanzdienstleister vor erhebliche operative und Compliance-Herausforderungen.

Finanzdienstleister mögen vielen anderen Branchen voraus sein, wenn es um ESG-Themen geht, aber diese werden in den kommenden Jahren durchaus ein wichtiger Risikofaktor sein. Soziale und ökologische Trends sind zunehmend Quellen für regulatorische Veränderungen und Haftung, zugleich werden eine verstärkte Offenlegung und Berichterstattung es künftig viel einfacher machen, Unternehmen und ihre Vorstände zur Verantwortung zu ziehen.

Ohnehin konzentrieren sich aktivistische Aktionäre oder Stakeholder zunehmend auf ESG-Themen. Die ersten Klimawandel-Klagen richten sich nun auch gegen Finanzinstitute. Bisher konzentrierten sich diese Fälle eher auf die Art der Geldanlagen, doch neuerdings zielen Klagen darauf ab, geschäftspolitische Veränderungen zu bewirken oder mehr Transparenz einzufordern. Neben dem Klimawandel gerät auch die soziale Verantwortung von Unternehmen ins Visier, wobei die Vergütung von Vorstandsgremien, Diversität in der Belegschaft und regulatorische Fragen besonders kritische Themen sind. Unternehmen, die sich Klimafreundlichkeit, Vielfalt und Inklusion auf die Fahnen schreiben, müssen Worten auch Taten folgen lassen. Diejenigen, die das nicht tun, werden die Folgen sehr bald spüren.

Covid-19 und die Auswirkungen

Als ob das alles nicht schon genügend Unsicherheiten im fragilen Risikomanagement-Gebilde vieler Banken sind, sorgt die Corona-Pandemie für zusätzliche Unsicherheit auf den Finanzmärkten: Covid-19 hat zweifelsohne einen der größten Schocks aller Zeiten für die Weltwirtschaft verursacht, der beispiellose wirtschaftliche und fiskalische Impulse und eine Rekordverschuldung der Regierungen ausgelöst hat. Trotz der verbesserten wirtschaftlichen Aussichten bleibt eine erhebliche Unsicherheit bestehen. Das Damoklesschwert der Wirtschafts- und Marktvolatilität schwebt weiter über uns – und die wirtschaftlichen Spätfolgen der Corona-Krise zeichnen sich bereits ab.

So steht eine Rekordverschuldung der Staaten als Erbe der Pandemie bereits fest. Größere Marktkorrekturen oder Ausschläge an den Märkten – etwa bei Aktien, Anleihen oder Krediten – könnten zu potenziellen Klagen von Anlegern und Aktionären führen. Zugleich könnte eine Zunahme von Insolvenzen von Unternehmen auch die eigenen Bilanzen der Institute zusätzlich belasten – die Zahl der kapitalschwachen „Zombi-Unternehmen" hat während der Pandemie zugenommen und das Auslaufen von staatlichen Unterstützungsmaßnahmen könnte eine nachgelagerte Insolvenzwelle auslösen.

Bereits im vergangenen Jahr waren die weltweiten Großinsolvenzen um 4 Prozent auf 422 Fälle gestiegen, im Vorjahr waren es noch 404. In Deutschland haben sich die großen Insolvenzen von 32 Fällen im Jahr 2019 auf 58 im Jahr 2020 nahezu verdoppelt, mit einem kumulierten Umsatz von mehr als 14 Milliarden Euro. Ein weiteres Covid-19-Risiko für Unternehmen: Es könnten vermehrt Ansprüche gegen Vorstände und leitende Angestellte geltend gemacht werden, wenn der Verdacht besteht, dass sie Risiken im Zusammenhang mit Covid-19 nicht vorhergesehen, offengelegt, gemanagt oder sich nicht darauf vorbereitet haben.

Krisenpläne ständig aktualisieren und testen

Wie kann der Finanzdienstleistungssektor diesen mannigfaltigen Herausforderungen begegnen? Ohne Zweifel haben die Institute in den vergangenen Jahren hart daran gearbeitet, ihr Risikomanagement zu verbessern. In den vergangenen Jahren gab es deutliche Fortschritte. Durch die Pandemie sind das Risiko- und ein gesamthaftes Business-Continuity-Management aber noch stärker in den Fokus der Unternehmen gerückt.

Viele Unternehmen haben in den vergangenen Monaten festgestellt, dass ihre Krisenpläne durch das schnelle Tempo der Pandemie und die Änderungen der öffentlichen Gesundheitsmaßnahmen schnell überfordert waren. Dies zeigt, dass Krisenpläne ständig aktualisiert und getestet werden müssen, damit sie am Tag X tatsächlich angewendet werden können. Sie müssen funktionsübergreifend sein und in das Risikomanagement und die strategischen Prozesse eines Unternehmens integriert sein.

Covid-19 hat zudem gezeigt, dass Unternehmen ein breiteres Spektrum an Szenarien in Betracht ziehen müssen, um auf zukünftige Schäden vorbereitet zu sein. Entscheidend ist deshalb mehr denn je ein vertiefter Risikodialog zwischen Versicherer und Versicherten und die Wahrnehmung der Leistungen im Bereich Schadenprävention, um gezielt Lösungen aus verschiedenen Versicherungssparten zusammenzuführen und in eine gezielte Risikomanagement-Strategie zu übersetzen. Dieser holistische Blick ist notwendig. Auch ohne Nick Leeson ist die Gefahr nicht gebannt.