BaFin Perspektiven

Ausgabe 1 | 2020

BaFin

Bundesamt
für Sicherheit in der
Informationstechnik

Cybersicherheit

Cybersicherheit

eine Herausforderung für Staat und Finanzwirtschaft

Inhaltsverzeichnis

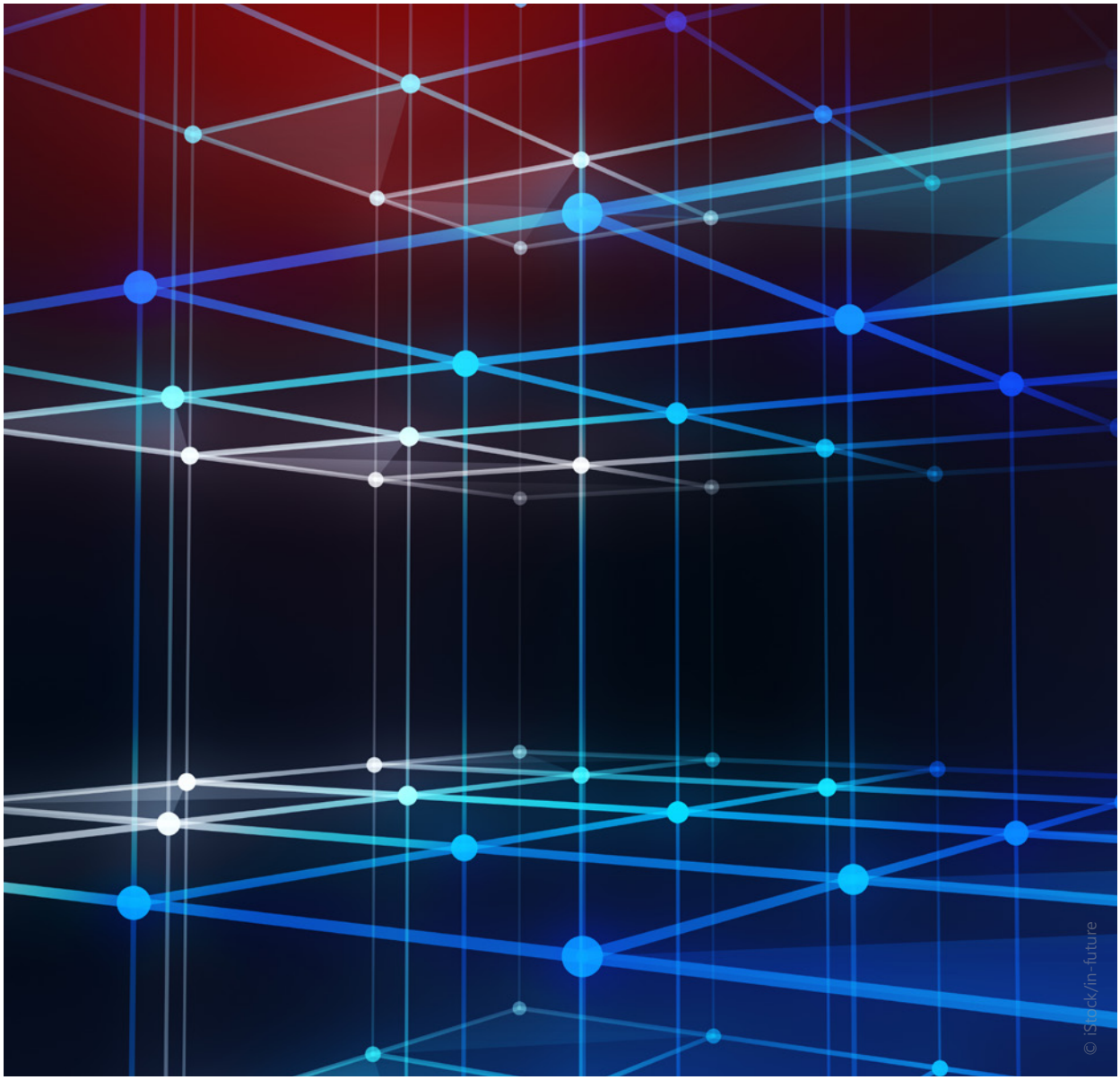
Aufsicht über Informationssicherheit und Cloud-Computing verlangt europaweite Harmonisierung 23

Für die BaFin als nationale Finanzaufsicht sind die Harmonisierung und Konvergenz aufsichtlicher Anforderungen an die Informationssicherheit und das Cloud-Computing auf nationaler und europäischer Ebene von großer Bedeutung. Auch die EU-Kommission und die europäischen Aufsichtsbehörden setzen sich immer stärker für eine Harmonisierung und Konvergenz der Aufsichtsstandards ein und tragen damit wesentlich zur Stärkung der operationalen digitalen Resilienz in der Europäischen Union bei. Ein Beitrag von Silke Brüggemann und Sibel Kocatepe

II. Cyber-Resilienz und Krisenmanagement – eine Aufgabe für Unternehmen und Aufsicht 34

Wie sich Deutschlands Banken gegen Cyberkriminalität rüsten 35

Cyberrisiken sind für die gesamte Kreditwirtschaft eine ernste Herausforderung. Kreditinstitute verfügen über eine große Expertise, ihre IT-Infrastrukturen zu schützen. Doch um den technischen Wettlauf gegen professionelle Cyberkriminelle auch künftig zu gewinnen, braucht es vor allem eins: eine stärkere internationale Zusammenarbeit. Banken, Sicherheitsindustrie sowie nationale und supranationale Behörden müssen an einem Strang ziehen. Ein Beitrag von Andreas Krautscheid und André Nash


© iStock/in-future

Vorwort

Ertragseinbußen in Millionenhöhe, schmerzhafte Arbeitsausfälle in Finanzunternehmen und am Ende steht sogar das Vertrauen der Kunden auf dem Spiel: Weltweit attackieren Cyberkriminelle IT-Schutzsysteme von Banken, Versicherern und anderen Finanzdienstleistern, um sich Zugriff auf sensible Daten wie Namen, Adressen, Telefonnummern, Passwörter und Kontonummern zu verschaffen. Erpresser schleusen Schadprogramme in IT-Systeme von Finanzunternehmen, fordern Lösegeld und drohen damit, die gesamte IT lahmzulegen. Szenarien wie diese sind alltäglich und verlangen daher die Aufmerksamkeit aller Mitarbeiter in Unternehmen sowie angemessene IT-Sicherheitsmaßnahmen.

Allein in Deutschland hat sich der gesamtwirtschaftliche Schaden durch Cyberkriminalität in den vergangenen zwei Jahren auf mehr als 100 Milliarden Euro verdoppelt, schätzt der Branchenverband Bitkom. Die Finanzbranche steht dabei besonders im Fokus von Cyberkriminellen. Fast täglich kommt es zu einem virtuellen Angriff auf ein Institut.

Der hohe Grad an Professionalisierung im Bereich Cybercrime macht es aus unserer Sicht notwendig, den Austausch zu diesem Thema noch weiter zu vertiefen und Akteure aus Wirtschaft und Staat miteinander zu vernetzen. Denn eine gute und vertrauensvolle Zusammenarbeit von der Prävention bis zum Krisenmanagement bei einem Cyberangriff ist unabdingbar, um die Widerstandsfähigkeit des Finanzstandorts Deutschland gegen Cybergefahren zu erhöhen.

Aus diesem Grund veröffentlichen wir, die Finanzaufsicht BaFin und das Bundesamt für Sicherheit in der Informationstechnik, BSI, diese Ausgabe der BaFinPerspektiven mit dem Titel „Cybersicherheit – eine Herausforderung für Staat und Finanzwirtschaft“ gemeinsam. Seit vielen Jahren arbeiten unsere beiden Bundesbehörden eng zusammen: Wir sprechen regelmäßig über die IT-Sicherheit in der Finanzbranche, tauschen uns über Technologietrends und Standardisierungen aus und beurteilen aktuelle Lagen. Beide Behörden bringen dabei ihre Expertise ein und lassen neue Erkenntnisse in die gemeinsame Arbeit im Hinblick auf kritische Infrastrukturen, KRITIS, einfließen, zu denen ein Teil der Banken, Versicherer und Dienstleister zählt.

Wir wünschen Ihnen eine interessante Lektüre!

Ihr Felix Hufeld
Präsident der BaFin

Ihr Arne Schönbohm
Präsident des BSI

I

Aktuelle Bedrohungslage und Diskussion über effektive Maßnahmen

Digital hilflos? Ein kurzer Überblick über die IT-Sicherheit in Deutschland

Autor

Tim Griese
Stv. Pressesprecher, Bundesamt für Sicherheit in der Informationstechnik (BSI)

1 Einleitung

In einer weiterhin angespannten IT-Sicherheitslage hat die Qualität vieler Cyberangriffe zugenommen.[1] Ein wesentliches Risiko für Staat, Wirtschaft und Gesellschaft geht von der Schadsoftware Emotet[2] aus, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits im Dezember 2018 als gefährlichste Schadsoftware der Welt bezeichnet hatte. Diese Einschätzung wurde durch die erheblichen Schäden bestätigt, die im Laufe des Jahres 2019 immer wieder durch Cyberangriffe mit Emotet entstanden sind. Betroffen waren unter anderem zahlreiche Universitäten, Krankenhäuser, Kommunen und Unternehmen, aber auch Privatanwender. Auch Finanzdienstleister gehörten zu den Zielen, sie konnten die Angriffe aber – soweit dem BSI ersichtlich – abwehren.

1 Dieser Beitrag basiert auf dem Bericht „Die Lage der IT-Sicherheit in Deutschland 2019“ des Bundesamts für Sicherheit in der Informationstechnik (BSI). Der Bericht enthält einen umfassenden und fundierten Überblick über die aktuelle Bedrohungslage im Cyberraum. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html;jsessionid=B335243B783E4AF950BE208C10C497C0.2_cid351, abgerufen am 7. April 2020.

2 Emotet ist ein Trojaner, der zum Beispiel Outlook-Kontakte und E-Mails ausspäht und Schadprogramme verteilt, indem die Spam-Mails als vermeintliche Antworten auf zuvor ausgespähte tatsächlich versandte E-Mails verschickt werden. Die bekannten Betreffzeilen und Zitate einer vorangegangenen Kommunikation lassen die gefälschten Mails für die Empfänger authentisch erscheinen.

2 Arten der Bedrohung

2.1 Ransomware

Auch unabhängig von Emotet zählt Ransomware nach wie vor zu den größten Bedrohungen – für Unternehmen, Behörden, andere Institutionen und Privatanwender. Immer wieder kommt es zu Komplettausfällen von Rechnern und Netzwerken, aber auch von Produktionsanlagen. Zudem sind im Laufe des Jahres 2019 auch Einrichtungen des Gemeinwesens wiederholt Ziel von Ransomware-Angriffen geworden. Dazu zählen Krankenhäuser und Kommunalverwaltungen. Dabei ist ein Trend zu beobachten: Angriffe richten sich gezielt gegen zentrale Dienstleister, über die dann deren Kundinnen und Kunden oder angeschlossene Netzwerke mit Ransomware infiziert werden können. Das Schadenspotenzial ist enorm: Die Kosten für Produktionsausfälle, Datenverlust sowie Bereinigung und Wiederherstellung der Systeme gehen zum Teil in die Millionen, Dienstleistungen von Einrichtungen des Gemeinwesens sind nicht oder nur eingeschränkt verfügbar.

2.2 Identitätsdiebstahl

Die vom BSI zuvor prognostizierte neue Qualität der Cyberangriffe drückt sich auch durch mehrere große Fälle von Identitätsdiebstahl aus, die in den Jahren 2018 und 2019 für Aufmerksamkeit sorgten. Unter anderem betroffen waren Anwender von Sozialen Netzwerken und Kunden großer Hotelketten sowie, im Zuge des im Januar 2019 bekannt gewordenen Doxing-Vorfalls, hunderte Prominente und Politiker aus Deutschland. Hunderte Millionen andere Internetnutzer mussten zusehen, wie ihre Daten unter den Überschriften „Collection #1“ bis „Collection #6“ öffentlich im Internet verfügbar gemacht wurden – ein gefundenes Fressen auch für weitere Cyberkriminelle. Bemerkenswert dabei ist nicht nur die Häufung der Vorfälle, sondern auch die riesige Menge der abgeflossenen und im Internet veröffentlichten persönlichen Daten.

2.3 Botnetze

Die Bedrohungslage durch Botnetze bleibt unverändert hoch, wobei sich auch hier die Angreifer die Digitalisierung zunutze machen und den Fokus auf mobile Endgeräte und Internet of Things (IoT)-Systeme legen. Täglich bis zu 110.000 Botinfektionen deutscher Systeme wurden 2019 registriert und vom BSI mit dem Ziel der Bereinigung an die jeweiligen Netzbetreiber gemeldet. Noch mehr Angriffspotenzial bergen serverbasierte Botnetze, insbesondere vor dem Hintergrund der zunehmend genutzten Cloud-Infrastrukturen. Mehr als jede zweite Attacke wird über kompromittierte oder missbräuchlich angemietete Cloud-Server ausgeführt. Fast jeder Cloud-Dienstleister wurde demnach bereits mindestens einmal von Kriminellen zur Durchführung von DDoS[3]-Attacken missbraucht.

2.4 Schadprogramme

Nach wie vor ist eine hohe Dynamik der Angreifer bei der (Weiter-)Entwicklung von Schadprogrammen und Angriffswegen festzustellen. Rund 114 Millionen neue Schadprogramm-Varianten wurden von Juni 2018 bis Mai 2019 identifiziert. Das Bedrohungspotenzial von Schadprogramm-Spam steigt weiterhin, auch wenn die Zahl der versendeten Spam-Mails gesunken ist. E-Mails mit Schadprogrammen zählen dennoch zu den am häufigsten detektierten Angriffen auf die Bundesverwaltung. Die Auswirkungen solcher Schadprogramme nehmen zu, nicht nur in der klassischen Bürokommunikation, sondern auch in Produktivbereichen der Wirtschaft.

Unnötig verschärft wird die ohnehin angespannte Cybersicherheitslage durch die in vielen Fällen festzustellende digitale Hilflosigkeit aufseiten der Anwender. Täter nutzen Schwächen individuellen Sicherheitsverhaltens in Verbindung mit strukturell unzureichend gesicherten Produkten und Systemen gezielt aus. Abhilfe kann die konsequente Nutzung von IT-Sicherheitsmaßnahmen nach Stand der Technik sowie eine Stärkung der digitalen Eigenverantwortung jedes einzelnen Nutzers schaffen.

3 Distributed Denial-of-Service.

3 Integrierte Wertschöpfungskette zum Schutz von Staat, Wirtschaft und Gesellschaft

Auch vor dem Hintergrund der angespannten Gefährdungslage kann die Digitalisierung hierzulande sicher gestaltet werden. Für einen starken und auch in Zukunft sicheren Standort Deutschland ist es notwendig, die Chancen der Digitalisierung aufzugreifen und zugleich den potenziellen Risiken von Beginn an angemessen zu begegnen. Deutschland als Wirtschafts- und Innovationsstandort muss Vorreiter einer Digitalisierung sein, die die Absicherung von IT-Produkten und auch von Unternehmensnetzwerken von vornherein mitdenkt und die Prinzipien Security-by-Default[4] und Security-by-Design[5] verinnerlicht hat.

Das BSI hat als Kompetenzzentrum des Bundes für IT- und Cybersicherheit dazu erfolgreich die Weichen gestellt und übernimmt Verantwortung bei dieser gesamtgesellschaftlichen Aufgabe. Das Amt beschäftigt sich täglich mit der Frage, in welchen Anwendungsfeldern der Digitalisierung Risiken entstehen könnten und wie sie kalkulierbar und beherrschbar gemacht werden können. Der Aufbau und die Bündelung von Know-how auf dem Gebiet der Cybersicherheit über einen Zeitraum von knapp 30 Jahren hat das BSI zu einer Behörde gemacht, in der die Fäden der Cybersicherheit zusammenlaufen. Aus den gewonnenen Erkenntnissen leitet das BSI jeweils passende Empfehlungen, Produkte oder Dienstleistungen für die unterschiedlichen Anforderungen von Staat, Wirtschaft und Gesellschaft ab. Diese integrierte Wertschöpfungskette der Cybersicherheit aus Prävention, Detektion und Reaktion unter einem Dach ist ein Alleinstellungsmerkmal des BSI.

4 Security-by-Default bedeutet, dass IT-Produkte und -Geräte in einem sicheren Zustand ausgeliefert werden müssen. Alle Sicherheitseinstellungen müssen so voreingestellt sein, dass der Anwender in Bezug auf die IT-Sicherheit möglichst keine Einstellungen mehr vornehmen muss.

5 Security-by-Design bedeutet, dass Sicherheit als explizite Anforderung in den Entwicklungsprozess eines Produktes aufgenommen wird und dass ganzheitliche Sicherheitsmaßnahmen von der Initialisierung an berücksichtigt, umgesetzt, getestet und vor Produktivsetzung fachlich abgenommen werden.

„Cyberkriminelle sind relativ faul“

Interview mit

Arne Schönbohm
Präsident, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Felix Hufeld
Präsident, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Selbst privat hatten sie bereits Ärger mit Hackern, geben beide Behördenchefs ehrlich zu. Arne Schönbohm und Felix Hufeld sprechen im Interview mit den BaFinPerspektiven im siebten Stock der BSI-Zentrale an der Godesberger Allee in Bonn über Lösungen gegen die Bedrohung aus dem Cyberspace.

Herr Hufeld, waren Sie selbst bereits Opfer eines Cyberangriffs?
Hufeld: Vor zehn Jahren erhielt ich eine angeblich unbezahlte Rechnung als Email auf mein privates Laptop. Über diese Behauptung war ich derart empört, dass ich aus Unerfahrenheit auf einen Link in der Mail klickte. Und zack hatte ich mir mit einem Erpressungstrojaner als Ransomware ein ernstes Problem eingehandelt. Der Bildschirm war blockiert und musste von einem teuren Computerprofi entsperrt werden. Das alles hat mich höllisch geärgert. Aber wenigstens habe ich keinen Erpresserlohn gezahlt. Seitdem passe ich besser auf.

Hatten Sie privat ähnlich böse Überraschungen, Herr Schönbohm?
Schönbohm: Auch ich wurde Anfang des Jahres Opfer mangelnder IT-Sicherheit – allerdings ohne eigenes Verschulden. Anfang des Jahres gab es einen Cyberangriff auf eine Autovermietung, bei der ich privat Kunde war. Dabei wurden viele persönliche Daten veröffentlicht, darunter meine Emailadresse und Telefonnummer. Auch Informationen wer, wo, wie, was gemacht hat, waren darunter. Im Anschluss habe ich per Email mehrere Phishing-Angebote bekommen, nach dem Motto „Sehr geehrter Herr Schönbohm, wir aktualisieren Ihre Kontodaten von der Sparkasse“. Der Absender war bei genauerem Hinsehen unseriös.

Wie schützen Sie sich gegen Gefahren im Cyberspace?
Hufeld: So simpel es klingt, so wirksam ist es. Ich schaue genau hin, was ich an Emails bekomme. Ich ändere regelmäßig meine Passwörter. Und ich installiere im privaten Umfeld – im dienstlichen tun wir das ja sowieso – hinreichende Abwehr- und Schutzsoftware, die zumindest das Gröbste ausfiltert. Doch manche Phishing-Mails kommen trotzdem durch. Dann hilft nur ein guter Instinkt.

Und was rät Deutschlands oberster Cyberschützer?
Schönbohm: Tatsächlich kann es immer zu einem erfolgreichen Cyberangriff kommen. Davor ist niemand gefeit. Daher ist es wichtig, frühzeitig eine Krisenreaktion vorzubereiten, damit der Schaden so gering wie möglich ausfällt. Ich rate bei privaten Fotos etwa zu Sicherheitskopien auf externen Festplatten. Bei einem Ransomware-Angriff kann man die Daten dann schnell wieder einspielen.

Datendiebstahl, Erpressung, Sabotage: Regelmäßig gibt es neue Fälle von Cyberkriminalität. Ist der Staat abwehrbereit?
Schönbohm: Ja, absolut. Die Cyberangriffe, denen auch die Bundesverwaltung ständig ausgesetzt ist, haben wir erfolgreich abgewehrt. Das liegt an unserer guten Netzinfrastruktur und dem IT-Sicherheitsgesetz, das 2015 verabschiedet wurde. Aber das ist auch immer ein Rennen zwischen Hase und Igel.

Ein Beispiel, bitte?
Schönbohm: Cyberangriffe mit breit angelegten Spam-Kampagnen wie der Schadsoftware Emotet oder die Angriffe über Schwachstellen von Citrix-Produkten waren vor wenigen Jahren noch nicht denkbar.

Wie steht Deutschland im internationalen Vergleich?
Schönbohm: In der Informationssicherheit sind wir gut aufgestellt. Deutschland hat es geschafft, in diesem Bereich ein Kompetenzzentrum aufzubauen: das BSI. Vorbildlich ist auch, dass wir unsere Informationen anderen wichtigen staatlichen Institutionen zur Verfügung stellen. So arbeiten wir für den Finanzbereich eng mit der BaFin und der Bundesbank zusammen.

Welches Land ist für Deutschland Vorbild?
Schönbohm: Deutschland orientiert sich stark an Frankreich mit seinen eher zentralen Strukturen. Beide Länder stehen in engem Austausch. Auch Israel ist hochspannend.

Warum?
Schönbohm: In Israel besteht ein enger Austausch zwischen den Sicherheitsbehörden, wie den israelischen Streitkräften, der Wissenschaft und der Wirtschaft. Japan ist wiederum stark bei Innovationen. Mit zahlreichen Ländern tauschen wir uns regelmäßig aus. Denn unser Ziel ist, von den Besten zu lernen.

Dem Klischee nach sind Hacker Typen im Kapuzenpullover, die im Dunkeln vor dem Computer sitzen. Stimmt das?
Schönbohm: Diese Hacker gibt es sicher immer noch, etwa in den fiktionalen Serien im Fernsehen oder bei den Streamingdiensten. Doch in der Realität gibt es auch solche, die sich der organisierten Kriminalität zurechnen lassen, die in der ganzen Welt operiert.

Welche Gruppen unterscheiden Sie?
Schönbohm: Da gibt es die Hacktivisten, die etwa mit einem Website-Defacement ein politisches Statement setzen wollen. In der Absicht, die Debatte um den Hambacher Forst zu beeinflussen, verändern sie beispielsweise Informationen auf der Homepage eines

Energiekonzerns. Andere Hacker greifen aus blanker Zerstörungswut kritische Infrastrukturen an. Und es gibt jene, die staatliche Institutionen oder Großkonzerne überfallen, um Schutzgeld zu erpressen – Stichwort Ransomware. Zudem gibt es auch technisch hochspezialisierte Hacker, die mit Methoden von Nachrichtendiensten versuchen, an Informationen zu gelangen.

Was sind neuralgische Angriffspunkte?
Schönbohm: Alles, womit sich Geld verdienen lässt. Und überall dort, wo man leicht eindringen kann. Cyberkriminelle sind relativ faul. Die Maxime ist: minimaler Einsatz, maximaler Erfolg. Umso wichtiger ist es, die Grundschutzmaßnahmen des BSI vollständig umzusetzen.

Welchen gesamtwirtschaftlichen Schaden verursacht Cyberkriminalität?
Schönbohm: Das Schadenspotenzial in Deutschland hat sich Schätzungen zufolge in den vergangenen zwei Jahren auf mehr als 100 Milliarden Euro verdoppelt. Doch wie lässt sich solch ein Schaden bemessen? Sind das Entwicklungskosten für ein neues Produkt? Ein entgangener Gewinn? Die verpasste Marktanteilspositionierung? Oder die Kosten für die Wiederherstellung der Systeme nach einer Attacke? Da müssen wir ein einheitliches Verständnis entwickeln.

Die Finanzbranche wird so häufig von Cyberkriminellen attackiert wie keine andere. Wie entwickeln sich die Fallzahlen?
Hufeld: Seit Jahresbeginn hat es eine erstaunliche Häufung von DDoS-Attacken auf Finanzinstitute gegeben. In den vergangenen zwei Jahren sind der BaFin insgesamt rund 600 Sicherheitsvorfälle gemeldet worden. Auch in den kommenden Jahren müssen wir mit steigenden Fallzahlen rechnen. Eines liegt auf der Hand: Banken, die schon in der guten alten Zeit Opfer von Überfällen waren, werden auch in einer virtuellen Welt attackiert.

Wie sehen diese Vorfälle aus?
Hufeld: Der Großteil der uns gemeldeten IT-Sicherheitsvorfälle ist kein Resultat externer Hackerangriffe, sondern Ergebnis interner Schwachstellen in den Instituten. Eine Verkettung merkwürdiger Umstände kann dabei zu signifikanten Schadensereignissen führen. Ich spüre noch immer eine gewisse Neigung, interne Schwachstellen und den berühmten menschlichen Faktor als Quelle von IT-Sicherheitsvorfällen zu unterschätzen.

Also sind meist die Mitarbeiter schuld?
Hufeld: Auch die kriminell motivierten externen Attacken nehmen zu. Und das Drama eines Angriffs von außen hat eine andere Brisanz, einen größeren Aufmerksamkeitswert. Aber die vielen kleinen Dummheiten des Alltags übersieht man dabei gerne. Und das wäre ein schwerer Fehler.

Banken, Versicherer und Finanzdienstleister, die bestimmte Kriterien erfüllen, gehören zu den Kritischen Infrastrukturen (KRITIS). Warum sind gerade dort Cyberangriffe so gefährlich?
Hufeld: Das Abwickeln von Finanztransaktionen ist der Blutkreislauf jeder Realwirtschaft. Wer dort mutwillig oder versehentlich eingreift, stoppt nicht nur einen abstrakten Geldfluss, sondern auch die dahinterstehenden realwirtschaftlichen Zusammenhänge. Das ist eine hochsensible Veranstaltung.

Wo liegen die Risiken?
Hufeld: Äußerst sensible, intime private Daten über einzelne Menschen, einzelne Familien, die man ungern in der Öffentlichkeit publiziert sehen möchte, werden dafür gespeichert. Um deren Willen möchte niemand erpresst werden. Hinzu kommt ein Spezifikum der Finanzwirtschaft: Cyberattacken treffen nicht nur einzelne Banken, Versicherer oder Finanzinstitute. Sondern die Verkettung der Institute kann relativ leicht zu systemischen Risiken führen. Das funktioniert etwa über Ansteckungskanäle, die extrem schwer zu kalkulieren sind.

Was ist in solchen Fällen die Folge?
Hufeld: Die Stabilität des gesamten Finanzsystems kann in Gefahr geraten. Dabei geht es um Vertrauen. Wenn Millionen Menschen in Panik geraten und sich dann die berühmten Schlangen vor Geldautomaten oder Bankschaltern bilden, muss das nicht zwingend auf harten Fakten beruhen. Es reichen Gerüchte. Das kann zu unglaublichen Aufstauungen und Wellen von menschlichem Verhalten führen. In manchen Ländern hat das zu systemischen Konsequenzen geführt. Die Finanzwirtschaft als kritische Infrastruktur muss daher besonders intelligent beschützt werden.

Ein DDoS-Angriff hat kürzlich das Online-Banking einer Direktbank stundenlang lahmgelegt. Haben Institute genug Know-how, sich zu schützen?
Hufeld: Theoretisch ja, aber in der Aufsichtspraxis sehen wir noch viel Luft nach oben. Was mich angesichts der jüngsten Vorfälle erschreckt hat: Selbst IT-Dienstleister, die hauptamtlich genau diese Dienste erbringen, lassen sich mit Leichtigkeit durch vergleichsweise simple technische Attacken aus der Bahn werfen. Das zeigen auch die meisten Ergebnissen der BaFin-Prüftätigkeiten in den Instituten. Obwohl die Industrie die Dimension der Herausforderung begriffen hat, muss noch viel getan werden. Gemütlich zurücklehnen können wir uns noch lange nicht.

Wie reagieren BaFin und BSI bei einem schweren Cyberangriff?
Schönbohm: BSI und BaFin informieren einander auf Arbeitsebene darüber, was genau geschehen ist, und geben eine Lageeinschätzung. Welcher Sachverhalt liegt vor, welche Unterstützungsleistung können wir dem betroffenen Institut anbieten? Ein Beispiel sind die Mobile Incident Response Teams.

Eine Art schnelle Eingreiftruppe?
Schönbohm: Ja. Die IT-Abteilung eines Unternehmens ist operativ meistens auf eine IT ausgelegt, die im Normalbetrieb funktioniert. Tritt eine Cyberattacke auf, so kann das immense Folgen haben, besonders dann, wenn sich das Institut auf den Krisenfall nicht vorbereitet hat. Prävention ist daher genauso wichtig wie Reaktion. Unsere Experten helfen dem betroffenen Konzern im akuten Fall: Wie lässt sich der Betrieb wiederherstellen? Wo finde ich einen Dienstleister, um Dateien wieder einzuspielen? Wie sieht die Krisenkommunikation aus?

Wie kontrollieren BaFin-Aufseher IT-Dienstleister der Finanzbranche?
Hufeld: Dass etliche Dienstleistungen im IT-Bereich über Auslagerungen und Outsourcing erbracht werden und nur zu einem geringen Teil hausintern, ist eher Regel als Ausnahme. Das ist auch völlig in Ordnung. Als Finanzaufseher achten wir bei auslagernden Finanzinstituten etwa darauf, dass im Vertrag mit dem Dienstleister bestimmte Qualitäts- und Überwachungsanforderungen berücksichtigt werden.

Besitzt die BaFin überhaupt direkten Zugriff auf die Dienstleister?
Hufeld: Die Situation ist derzeit heterogen. Interessanterweise hat die BaFin aus der Historie heraus sehr weitreichende Zugriffsrechte in der Versicherungsaufsicht. In der Bankenaufsicht haben wir dagegen weniger Möglichkeiten. Inwieweit wir hier angesichts der immer größeren Bedeutung von Outsourcing für das gesamte Finanzsystem darauf regulatorisch reagieren müssen, etwa, indem wir den traditionellen aufsichtsrechtlichen Bezug ausdehnen, wird diskutiert werden müssen. Ich halte eine solche Diskussion jedenfalls für geboten und sie hat auch in den internationalen regulatorischen Gremien bereits begonnen.

Vor der Coronakrise schätzten Konzerne laut Risiko-Barometer 2020 der Allianz den Cyberbetrug als ihr wichtigstes Geschäftsrisiko ein. Teilen Sie den Eindruck aus der Aufsichtspraxis?
Hufeld: Ja, die Bedrohungslage ist inzwischen im allgemeinen Bewusstsein. Ich kann mir nur noch sehr wenige Bankvorstände vorstellen, die nicht grundsätzlich anerkennen, dass im IT-Bereich erhebliche Risiken bestehen. Informationssicherheit ist als Risikomanagement Chefsache. Immerhin ist das Finanzinstitut im schlimmsten Fall im Bestand bedroht.

Handeln Finanzmanager auch danach?
Hufeld: Ob dieses Thema Tag für Tag, Woche für Woche tatsächlich hinreichend gemanagt wird? Nein. Da sind wir von einem zufriedenstellenden Niveau noch eine gute Wegstrecke entfernt.

Konzerne machen das Problem der Cyberkriminalität ungern öffentlich. Zurecht?
Schönbohm: Nein, diese Strategie ist falsch. Wenn es in einem Finanzinstitut zu einem Cybervorfall kommt, ist es wichtig, sich unmittelbar an das BSI oder die BaFin zu wenden. Alle Informationen werden vertraulich behandelt. Am schlimmsten ist es, wenn Unternehmen versuchen, Attacken zu vertuschen. Oft gehen Cyberkriminelle ähnlich vor und suchen sich verschiedene Opfer der gleichen Branche. Wenn wir informiert sind, können wir andere frühzeitig warnen.

Unabhängig vom akuten Cyberangriff nehmen BaFin-Aufseher regelmäßig Prüfungen der hauseigenen IT bei Instituten ab? Warum?
Hufeld: Die Fähigkeit zum störungsfreien Ablauf einer Geschäftsorganisation ist eine Grundvoraussetzung funktionierender Finanzinstitute – ähnlich wie etwa die Kapitalausstattung und das Liquiditätsmanagement. Die Finanzwirtschaft hängt so stark, wie man es sich nur vorstellen kann, von einer funktionierenden IT ab. Deshalb muss das ein zentraler Bestandteil jeder klassischen Prüf- und Aufsichtstätigkeit sein.

Wie gehen Sie dabei vor?
Hufeld: Als Finanzaufsicht haben wir zuerst klar formuliert, was wir von den Instituten erwarten. Zuerst haben wir die berühmten Bankaufsichtlichen Anforderungen an die IT-Sicherheit (BAIT) systematisch entwickelt, dann die Anforderungen für die Versicherungsindustrie (VAIT) und schließlich für Kapitalanlagegesellschaften (KAIT).

Und sonst?
Hufeld: Wir haben unsere eigene Fähigkeit deutlich gestärkt, die IT-Sicherheit vor Ort zu prüfen. Dafür haben wir spezialisierte Strukturen innerhalb der BaFin aufgebaut. Inzwischen ist es ein klassischer Bestandteil unserer Aufsichts- und Prüftätigkeit. Hinzu kommt, dass die BaFin auch verstärkt die Resilienz von Unternehmen testet. Momentan setzen wir die europäischen Rahmenvorgaben, TIBER-EU, in die Realität um. Auch bereiten wir uns auf akute Schadensereignisse in Instituten vor.

Auch gegen Cyberschäden gibt es Versicherungen. Wie steht es um deren Risikobewertung?
Hufeld: Cyberrisiken sind ein vergleichsweise neues Phänomen, das in unterschiedlichen Erscheinungsformen derzeit auch Versicherer zu recht auf Trab hält. Bei der Erstellung neuer Produkte wie Cyberpolicen müssen Versicherungen, die seit Jahrhunderten üblichen Grundparameter beachten. Der Deckungsumfang, der Rückversicherungsschutz sowie die Tarifierungsmerkmale und schadenauslösende Faktoren sind bei der Kalkulation eines neuen Risikos wichtig.

Könnten nicht auch in älteren Policen Cyberrisiken schlummern?
Hufeld: Tatsächlich hatte ich Sorge, dass bei Versicherern in puncto Cyberrisiko querbeet versteckte Tretminen bestehen. Deshalb untersuchte die BaFin im engen Austausch mit der Branche, ob in alten Deckungswerken und Policen solche Gefahren lauerten. Schließlich können sogenannte Silent Cyber Risks, falls sie schlagend werden, ein großes Schadensereignis auslösen.

Was fanden Sie heraus?
Hufeld: Wir hatten den Verdacht, dass mancherorts das Risiko nicht angemessen tarifiert wird – zum Beispiel, weil es der Versicherer vor etlichen Jahren, als er das in die Deckung genommen hat, noch gar nicht auf dem Radar hatte. Diese Sorge hat sich allerdings kaum bestätigt. Das Ergebnis unserer Untersuchung hat mich beruhigt.

Online-Banking, digitales Bezahlen, interne Prozesse: Die Digitalisierung bot Finanzinstituten zuletzt Chancen, Geschäftsmodelle umzubauen. Setzt ihnen die Cyberkriminalität jetzt am Ende die Grenzen?
Hufeld: Nein, eine absolute Innovationsgrenze sehe ich nicht. Ich bin Optimist. Und daher glaube ich an die Innovationsfähigkeit der Menschen, der Industrie und der Politik. Wohin sich die Digitalisierung in den kommenden Jahren auch entwickeln mag, wir werden Antworten finden. Es gibt eine immerwährende Abwägung zwischen den Zielen der Innovation, der Schnelligkeit und des Komforts einerseits sowie Sicherheit andererseits. All die schönen Dinge, die wir wollen, müssen in einem sicheren Umfeld gelingen, und beides steht in Spannung zueinander. Angesichts dieser klassischen „Public Policy Choices" ist es unsere Aufgabe als Behörden, der Politik Vorschläge zu unterbreiten, wie sich unterschiedliche aber völlig legitime politische Ziele in vernünftiger Abgewogenheit erreichen lassen.

Herr Schönbohm, teilen Sie diesen Optimismus?
Schönbohm: Ja, absolut. Ich glaube, wir sind in Deutschland deutlich besser, als wir uns manchmal selbst machen. Estland gilt etwa als leuchtendes Vorbild in puncto IT-Sicherheit, die aber letztlich auf deutschem Know-how wie etwa dem IT-Grundschutz des BSI basiert. Im weltweiten Vergleich stellt Deutschland die meisten Informationssicherheits-Zertifizierungen im Hochsicherheitsbereich aus. Als Nation und Unternehmerland kombinieren wir in Deutschland zwei Dinge: Offen sein und digital denken. In Verbindung mit dem richtigen Maß an Informationssicherheit sind das hervorragende Voraussetzungen, um die Digitalisierung erfolgreich zu gestalten.

Herr Schönbohm, Herr Hufeld, vielen Dank für das Interview.
Die Fragen stellte Annkathrin Frind, BaFin, Gruppe Kommunikation.

Zur Person
BSI-Präsident Arne Schönbohm

Der Behördenchef Seit 2016 ist Arne Schönbohm Präsident des Bundesamts für Sicherheit in der Informationstechnik, (BSI). Zuvor war er Präsident des Cyber-Sicherheitsrats e.V. und arbeitete als Berater für IT-Sicherheit. Der Betriebswirt studierte Internationales Management in Dortmund, London und Taipeh. Schönbohm begann seine berufliche Karriere bei DaimlerChrysler Aerospace. Anschließend hatte er führende Positionen bei EADS inne.

Die Behörde Das Bundesamt für Sicherheit in der Informationstechnik (BSI) untersteht als zentraler IT-Sicherheitsdienstleister des Bundes dem Bundesinnenministerium. Die Bonner Behörde ist für die Sicherheit der Netze des Bundes sowie für den Schutz kritischer Infrastrukturen zuständig.

Zur Person
BaFin-Präsident Felix Hufeld

Der Behördenchef Felix Hufeld ist seit 2015 Präsident der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Zuvor war er als Exekutivdirektor für die Versicherungsaufsicht zuständig. Der Jurist hat in Mainz, Freiburg und Harvard studiert. Seine Karriere begann er bei der Unternehmensberatung Boston Consulting. Anschließend arbeitete er unter anderem für die Dresdner Bank und den Versicherungsmakler Marsh.

Die Behörde Die BaFin kontrolliert Banken, Finanzdienstleister, Versicherer und den Wertpapierhandel. Sie ist eine Anstalt des öffentlichen Rechts und unterliegt der Rechts- und Fachaufsicht des Bundesfinanzministeriums.

Aufsicht über Informationssicherheit und Cloud-Computing verlangt europaweite Harmonisierung

Autor

Silke Brüggemann
Referentin, Referat Grundsatz IT-Aufsicht und Prüfungswesen, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Sibel Kocatepe
Referentin, Referat Grundsatz IT-Aufsicht und Prüfungswesen, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

1 Einleitung

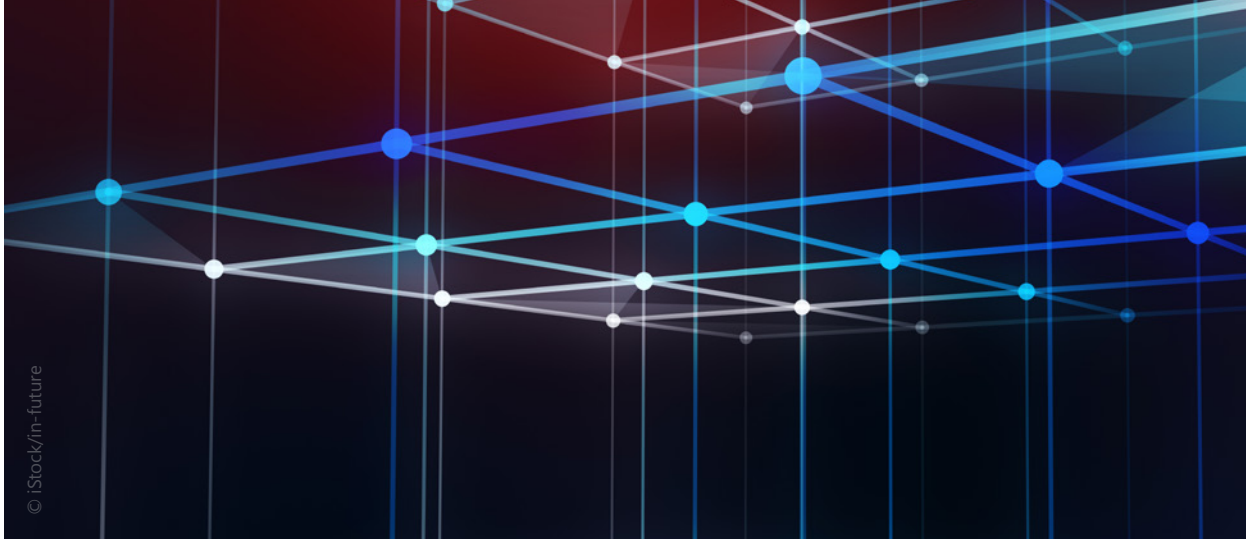
Die Harmonisierung und Konvergenz aufsichtlicher Anforderungen an Finanzunternehmen ist die Grundlage für einen stabilen Finanzmarkt und eine Stärkung der digitalen operationalen Resilienz des Finanzsektors. Aus diesem Grund hat die EU-Kommission dieses politische Vorhaben in den Fokus gerückt: Mit dem abgeschlossenen FinTech-Aktionsplan[1] (siehe Infokasten, Seite 26) will sie einen wettbewerbsfähigen, innovativen – aber auch sicheren – europäischen Finanzsektor schaffen. Die EU-Kommission hat ihre Überlegungen zu den hierfür wichtigen Bereichen Informationssicherheit und Cloud-Computing im Dezember 2019 mit der Initiative „Finanzdienstleistungen – Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen (neue Vorschriften)“[2] konkretisiert.

Anfang April 2020 hat die EU-Kommission eine sich ebenfalls an den oben genannten FinTech-Aktionsplan anschließende „Consultation on a new digital finance strategy for Europe / FinTech action plan“[3] veröffentlicht. Die Ergebnisse dieser öffentlichen Konsultation, die am 26. Juni 2020 endet, fließen in eine neue fünfjährige digitale Finanzstrategie / einen neuen FinTech-Aktionsplan ein. Wohingegen sich die im Dezember 2019 veröffentlichte Konsultation dem Thema digitale operationale Resilienz annimmt, blickt diese Konsultation auf die Themen Sicherstellung der Technikneutralität und Innovationsfreundlichkeit ohne dabei den Verbraucherschutz aus den Augen zu verlieren, die Beseitigung der Fragmentierung für digitalen Finanzdienstleistungen im europäischen Wirtschaftraum und Förderung eines angemessen regulierten datengetriebenen Finanzsektors. Mit der für das dritte Quartal 2020 geplanten Veröffentlichung dieser digitalen Finanzstrategie / dieses FinTech-Aktionsplans will die EU-Kommission die Herausforderungen der fortschreitenden Digitalisierung adressieren und die Innovationskraft des europäischen Finanzsektors stärken.

1 EU-Kommission, FinTech-Aktionsplan: Für einen wettbewerbsfähigen und innovativeren EU-Finanzsektor, https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-109-F1-DE-MAIN-PART-1.PDF, abgerufen am 10.3.2020.

2 EU-Kommission, Finanzdienstleistungen – Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen (neue Vorschriften), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act, abgerufen am 6.5.2020.

3 EU-Kommission, Consultation on a new digital finance strategy for Europe / FinTech action plan, https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_de, abgerufen am 21.4.2020.



Unter Bezugnahme auf diese Entwicklungen gibt dieser Artikel einen Überblick über den aktuellen Stand der deutschen und europäischen Harmonisierungsbestrebungen im Bereich der Informationssicherheit (inklusive Cybersicherheit) und des Cloud-Outsourcings, erhebt dabei aber keinen Anspruch auf Vollständigkeit. Die Darstellungen beschränken sich auf öffentlich zugängliche Informationen, die von Aufsichtsbehörden und europäischen Institutionen des Finanzsektors stammen. Nicht-öffentliche Informationen, insbesondere zu Aufsichtspraktiken, sind aufgrund ihrer Vertraulichkeit in diesem Artikel nicht aufgeführt.

Ein Überblick zu weltweiten Regulierungen im Bereich der Informationssicherheit ist im nachstehenden Infokasten aufgeführt.

Auf einen Blick

Internationale Veröffentlichungen zu Anforderungen an die Informationssicherheit

Einen allgemeinen Überblick zu internationalen Regularien liefert der Finanzstabilitätsrat FSB (Financial Stability Board) im Dokument „Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices"[4] aus dem Jahr 2017.

Weltweite Praktiken im Bankensektor fasst der Basler Ausschuss für Bankenaufsicht BCBS (Basel Committee on Banking Supervision) in seiner Publikation „Cyber-resilience: Range of practices"[5] aus dem Jahr 2018 zusammen.

Für den Versicherungssektor gibt das „Application Paper on Supervision of Insurer Cybersecurity"[6] (November 2018) der Internationalen Vereinigung der Versicherungsaufsichtsbehörden IAIS (International Association of Insurance Supervisors) eine entsprechende Übersicht.

Für Finanzmarktinfrastrukturen liefert die Cyber Task Force der Internationalen Organisation der Wertpapieraufsichtsbehörden IOSCO (International Organization of Securities Commissions) in ihrem Final Report[7] eine vergleichbare Analyse.

4 FSB, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, https://www.fsb.org/wp-content/uploads/P131017-2.pdf, abgerufen am 12.1.2020.

5 BIS, Cyber-resilience: range of practices, https://www.bis.org/bcbs/publ/d454.pdf, abgerufen am 16.12.2019.

6 IAIS, Application paper on Supervision of Insurer Cybersecurity, https://www.iaisweb.org/file/77763/application-paper-on-supervision-of-insurer-cybersecurity, abgerufen am 12.1.2020.

7 IOSCO, Cyber Task Force – Final report, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf, abgerufen am 12.1.2020.

2 Harmonisierung regulatorischer Anforderungen in Deutschland: BAIT, VAIT und KAIT

Die BaFin hat mit ihren Bankaufsichtlichen Anforderungen an die IT (BAIT)[8] im Jahr 2017, ihren Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) [9] im Jahr 2018 und ihren Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT)[10] im Jahr 2019 im internationalen Vergleich frühzeitig deutlich gemacht, wie beaufsichtigte Finanzunternehmen ihre Geschäftsorganisation im Hinblick auf Informationssicherheit ordnungsgemäß gestalten sollen.

Diese drei Rundschreiben bilden den zentralen Baustein der Aufsicht über die Informationssicherheit. Zugleich adressiert die BaFin darin wesentliche Mängel, die sie bei IT-Prüfungen von Finanzunternehmen in den vergangenen Jahren entdeckt hat. Gemeinsames Ziel ist, einen verständlichen wie flexiblen Rahmen für das Management der Informationssicherheit zu schaffen, das unternehmensweite Bewusstsein zu schärfen und den Geschäftsleitungen der Finanzunternehmen die Erwartungen der Finanzaufsicht hinsichtlich einer angemessenen Informationssicherheit – in den Finanzunternehmen und gegenüber Drittanbietern – transparent zu machen.

Finanzunternehmen sind verpflichtet, eine ordnungsgemäße Geschäftsorganisation zu gewährleisten. Die drei Rundschreiben mit ihren aufsichtlichen Anforderungen an die Informationssicherheit sollen den Unternehmen Klarheit und Sicherheit in Bezug auf Anforderungen betreffend die IT-Strategie, die IT-Governance, das Informationsrisiko- und Informationssicherheitsmanagement sowie die Auslagerung (Outsourcing) von Dienstleistungen geben.

Auch technische Aspekte der Informationssicherheit umfassen die Rundschreiben, zum Beispiel mit Anforderungen zum Benutzerberichtigungsmanagement, zu IT-Projekten, zur Anwendungsentwicklung und zum IT-Betrieb. Dabei bleiben sie allerdings technologieneutral.[11]

Finanzunternehmen sollen die Anforderungen prinzipienorientiert umsetzen und dabei das Prinzip der Proportionalität berücksichtigen. Die BaFin verfolgt insgesamt einen konvergenten und harmonisierten Regulierungs- und infolgedessen Aufsichtsansatz. Aus diesem Grund verwendet sie in allen drei Rundschreiben identische Fachbegriffe. Trotzdem berücksichtigt sie auch sektorspezifische Besonderheiten. Beispiele sind die jeweiligen Bezugnahmen in BAIT und KAIT auf die entsprechenden Mindestanforderungen an das Risikomanagement von Instituten (MaRisk) oder von Kapitalverwaltungsgesellschaften (KAMaRisk) sowie das KRITIS-Modul in BAIT und VAIT.

8 Vgl. BaFinJournal Januar 2018, und BaFinPerspektiven Seite 17 ff. und BaFin, Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT), www.bafin.de/dok/10171052, abgerufen am 6.5.2020.

9 Vgl. BaFinJournal April 2018, Seite 24 ff. und BaFin, Rundschreiben 10/2018 – Versicherungsaufsichtliche Anforderungen an die IT (VAIT), www.bafin.de/dok/11102952, abgerufen am 6.5.2020.

10 BaFin, Rundschreiben 11/2019 (WA) – Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT) vom 1.10.2019, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1911_kait_wa.html, abgerufen am 6.5.2020.

11 Vgl. Aufsichtsschwerpunkte der BaFin 2020, Seite 9, www.bafin.de/dok/13482592, abgerufen am 6.5.2020.

3 Harmonisierung regulatorischer Anforderungen an die IT-Sicherheit von Finanzunternehmen in Europa

Mit der Veröffentlichung des FinTech-Aktionsplans[12] (siehe Infokasten) hat die EU-Kommission die drei Europäischen Aufsichtsbehörden (European Supervisory Authorities – ESAs) aufgefordert, gemeinsame Vorschläge zu entwickeln, wie Unternehmen aus dem Finanzsektor ihre Cyber-Resilienz (siehe Infokasten) stärken und verbessern können.

Auf einen Blick

FinTech-Aktionsplan

Die EU-Kommission hat im März 2018 ihren Aktionsplan für einen wettbewerbsfähigen und innovativen Finanzsektor in Europa veröffentlicht. Ziel ist, dass Finanzunternehmen technologisch getriebene Innovationen besser nutzen. Die Kommission will mit den im Aktionsplan beschriebenen Maßnahmen innovative Geschäftsmodelle fördern und Finanzunternehmen darin bestärken, neue Möglichkeiten wie Distributed-Ledger-Technologien und Cloud-Dienste zu nutzen. Als dritte Maßnahme und primäres Ziel des Aktionsplans steht die Verbesserung der Cyber-Resilienz der Finanzunternehmen im Fokus.

Auf einen Blick

Cyber-Resilienz

Cyber-Resilienz bezeichnet die Widerstandsfähigkeit von Unternehmen bei Angriffen auf die Sicherheit ihrer Informations- und Kommunikationstechnik (IKT). Im Fokus der Angreifer stehen die Systeme der Unternehmen oder auch die Daten von Kunden.

12 a.a.O. (Fn. 1).

Dieser Aufforderung sind die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung EIOPA (European Insurance and Occupational Pensions Authority), die Europäische Bankenaufsichtsbehörde EBA (European Banking Authority) und die Europäische Wertpapier- und Marktaufsichtsbehörde ESMA (European Securities and Markets Authority) in ihrer Stellungnahme „Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements“ [13], die sie Anfang April 2019 gemeinsam veröffentlicht haben, nachgekommen. Darin schlagen die ESAs der EU-Kommission konkrete Maßnahmen zur Harmonisierung und Konvergenz von Anforderungen an die Sicherheit der Informations- und Kommunikationstechnologie (IKT) der Finanzunternehmen vor.[14]

Wo Harmonisierungsbedarf besteht

Unter anderem am Beispiel des europäischen Versicherungssektors haben die ESAs in ihrer Stellungnahme den notwendigen Harmonisierungsbedarf aufgezeigt: Obwohl zum Zeitpunkt einer von EIOPA vorgenommenen Umfrage 22 von 28 EWR Mitgliedsstaaten Gesetze und/oder Anforderungen zu Informationssicherheit haben, zeigen sich erste Unterschiede bereits bei der rechtlichen Verbindlichkeit der veröffentlichten Anforderungen. Diese sind in einem Spektrum von Gesetzen, Rundschreiben, Leitlinien/-fäden oder Mischformen verfasst.

Thematisch behandelt die Mehrheit an Dokumenten Anforderungen zu den Hauptgebieten der Informationssicherheit. Dazu gehören die IT-Strategie, Informationsrisikomanagement, das Informationssicherheitsmanage-

13 Joint Committee – European Supervisory Authorities, Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements - JC 2019 26, https://eiopa.europa.eu/Publications/JC%202019%2026%20(Joint%20ESAs%20Advice%20on%20ICT%20legislative%20improvements).pdf , abgerufen am 10.3.2020.

14 Vgl. BaFinJournal April 2019, Seite 26 ff.

ment, der IT-Betrieb und das Outsourcing-Management. Details und einzelne Aspekte der unterschiedlichen Anforderungen variieren dabei allerdings stark.

Die Themen „Malware, Patch- und Anti-Virus-Management", „Schulungen zur Informationssicherheit" und IT-Governance decken die Veröffentlichungen der EWR-Mitgliedsstaaten dahingegen nur zu knapp 50 Prozent ab.

Insgesamt zeigt die Erhebung von EIOPA ein weites Spektrum an nationalen regulatorischen Anforderungen mit unterschiedlichen Inhalten sowie voneinander abweichender Detailtiefe und rechtlicher Verbindlichkeit. Um dieser Heterogenität zu begegnen, kündigt EIOPA in der Stellungnahme der ESAs an, Leitlinien für die Informationssicherheit zu entwickeln. Mit diesem Schritt folgt sie der EBA, die bereits Ende 2018 ihren Leitlinienentwurf zur Konsultation gestellt hat.[15] Die ESMA arbeitet zwar derzeit nicht an eigenen Anforderungen an die Informationssicherheit, fördert aber den Informationsaustausch zwischen nationalen Aufsichtsbehörden in Bezug auf Cyberrisiken.[16]

Letztendlich sehen die ESAs für alle Sektoren, was Anforderungen an die Informationssicherheit betrifft, Harmonisierungs- und Ergänzungsbedarf. Nach Ansicht der ESAs trägt eine sektorübergreifende Harmonisierung der Anforderungen an die Geschäftsorganisation zum Beispiel zu einem insgesamt höheren Sicherheitsniveau, zu angemessenen Aufsichtspraktiken auf dem Gebiet der Informationssicherheit und zu einer besseren Cybersicherheit bei.

Konsequenterweise schlagen daher die ESAs der EU-Kommission vor, die einschlägigen europäischen Richtlinien um Aspekte der Informationssicherheit zu ergänzen, um in allen Finanzsektoren das gleiche Ausgangsniveau herzustellen. Diesen Vorschlag hat die EU-Kommission in ihrem Konsultationsdokument „A potential initiative on the digital operational resilience in the area of financial services" [17] im Rahmen ihrer Initiative „Finanzdienstleistungen – Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen (neue Vorschriften)"[18] aufgegriffen, das sie im Dezember 2019 veröffentlicht hat. Mittels eines Fragebogens eruierte die EU-Kommission bis Mitte März 2020 bei Stakeholdern aus unterschiedlichen Bereichen, wie sie zu einer weitergehenden Harmonisierung unter anderem von Anforderungen im Bereich der Informationssicherheit zur Erhöhung der digitalen operationalen Resilienz [19] im Finanzsektor stehen. Die Konsultationsergebnisse veröffentlichte die EU-Kommission noch nicht. Erste Schritte hierzu haben die ESAs bereits mit ihren Veröffentlichungen im Bereich der Informationssicherheit umgesetzt.

Leitlinien für mehr Informationssicherheit in Europa

Die EBA hat Ende November 2019 ihre finalen Leitlinien für das Management von IKT- und Sicherheitsrisiken[20] veröffentlicht[21]. In ihren Leitlinien, die sich an Finanzinstitute und Zahlungsdienstleister richten, legt die EBA „die Maßnahmen für das Management von Risiken fest, die Finanzinstitute (wie in Absatz 9 unten festgelegt) gemäß

15 Vgl. BaFinJournal Dezember 2019, Seite 11.

16 ESMA, ESA Review, https://www.esma.europa.eu/about-esma/who-we-are/esa-review, abgerufen am 20.1.2020.

17 EU-Kommission, Consultation document: A potential initiative on the digital operational resilience in the area of financial services, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf, abgerufen am 7.1.2020.

18 a.a.O. (Fn. 2).

19 a.a.O. (Fn. 18)

20 EBA, EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880810/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_DE.pdf , abgerufen am 10.3.2020.

21 EBA, Press release: EBA publishes guidelines on ICT and security risk management, https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management, abgerufen am 6.5.2020.

Artikel 74 der CRD für die Verwaltung ihrer IKT- und Sicherheitsrisiken für alle Tätigkeiten ergreifen müssen und die Zahlungsdienstleister (ZDL, wie in Absatz 9 festgelegt) gemäß Artikel 95 Absatz 1 der PSD2, übernehmen müssen, um die operationellen und sicherheitsrelevanten Risiken („IKT- und Sicherheitsrisiken") in Bezug auf die von ihnen erbrachten Zahlungsdienste zu beherrschen. Die Leitlinien umfassen Anforderungen an die Informationssicherheit, einschließlich Cybersicherheit, soweit die Informationen auf IKT-Systemen gehalten werden."[22]

Auch EIOPA hat, wie in der gemeinsamen Stellungnahme der ESAs angekündigt, Ende 2019 einen Entwurf zu Leitlinien für IKT-Governance und -Sicherheit zur Konsultation gestellt[23] und wertet aktuell die Antworten zu der im Marz 2020 beendeten öffentlichen Konsultation aus. Die Leitlinien richten sich an Versicherungsunternehmen und -gruppen, für die das Solvency-II-Regime gilt. Sie folgen insgesamt, in dem bei ihrer Erstellung auf dem Leitlinienentwurf der EBA aufgesetzt wurde, dem in der gemeinsamen Stellungnahme vorgeschlagenen harmonisierten Regulierungsansatz und führen damit den schon bei den BAIT, VAIT und KAIT eingeschlagenen Weg der Harmonisierung der Anforderungen fort.

Beide Fassungen an Leitlinien behandeln zwar die gleichen Aspekte der Informationssicherheit, variieren aber in der Detailtiefe und weisen Abweichungen in der Formulierung der Anforderungen auf. Dies ist durch Spezifika der jeweiligen Regulierungen, regulatorische Herangehensweisen und Unterschieden in den Risikoprofilen der jeweiligen Unternehmen bedingt[24].

Letzteres ist auch der Grund dafür, warum EIOPA das Informationssicherheitsziel der „Verfügbarkeit"[25] in ihren Leitlinienentwurf anders behandelt als die EBA in ihren finalen Leitlinien. Im Vergleich zu anderen Akteuren des Finanzsektors wie Finanzinstituten oder Zahlungsdienstleistern sind Versicherer, insbesondere Kranken- und Lebensversicherungsunternehmen, weniger vulnerabel in Bezug auf Betriebsunterbrechungen oder disruptiven Attacken. Beispielsweise ist es für Versicherer, im Vergleich zu der Verfügbarkeit von Zahlungsdiensten weniger zeitkritisch, die Verfügbarkeit vieler Bereiche ihres Unternehmens wiederherzustellen[26].

Allgemein heben die Leitlinien von EBA und EIOPA die Gesamtverantwortung der Geschäftsleitung, eine ausreichende Ressourcen- beziehungsweise Budgetausstattung und das Prinzip der Proportionalität in den Anforderungen an die Informationssicherheit hervor. Im Bereich der Governance bekräftigen beide, die Informationssicherheit in der Geschäftsorganisation, in der Unternehmensstrategie, im Gesamtrisikomanagement, beim Outsourcing und im Audit seitens der jeweiligen Unternehmen zu berücksichtigen.

Ausführlich stellt die EBA ihre Anforderungen dar, wie die Informationssicherheitsrisiken im Gesamtrisikomanagement zu berücksichtigen sind. Während EIOPA in ihrer Leitlinie zum Risikomanagement primär auf die Schutzbedarfsfeststellung eingeht, erläutert die EBA in ihrem Abschnitt „Rahmenwerk für das Management von IKT- und Sicherheitsrisiken" der Leitlinien detailliert die Vorgehensweise beim IKT- und Informationssicherheitsrisikomanagement inklusive der Schutzbedarfsfestellung im Rahmen des Gesamtrisikomanagements. Diese unterschiedliche Herangehensweise fußt auf dem Ansatz von EIOPA, sich bei ihren Ausführungen zu Governance-Anforderungen wesentlich auf Aspekte der Informationssicherheit zu konzentrieren und demzufolge allgemeine Governance-Anforderungen in ihren Leitlinien nicht zu wiederholen. Das zeigt sich in gleicher Art und Weise auch in den Ausführungen zum Audit.

Die Ausführungen zur Informationssicherheitsleitlinie der EBA und der entsprechenden Leitlinie von EIOPA legen übergeordnete Grundsätze und Regeln fest, um die

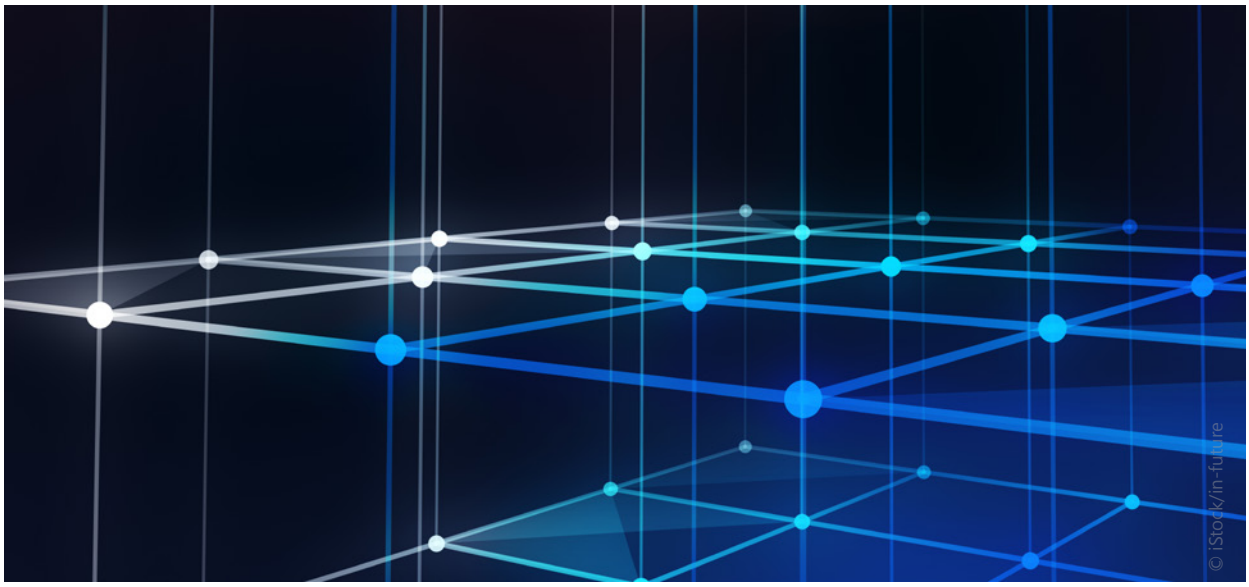
22 a.a.O. (Fn. 21), Seite 6.

23 EIOPA, Consultation paper on the proposal for Guidelines on Information and Communication Technology (ICT) security and governance, https://www.eiopa.europa.eu/sites/default/files/publications/consultations/guidelines_ict_security_and_governance_12122019_for_consultation.pdf, abgerufen am 6.5.2020.

24 a.a.o. (Fn. 14), JC 2019 26, Seite 28ff: Annex B2. ICT security risk profile of an insurance or reinsurance undertaking.

25 Verfügbarkeit: „Property of being accessible and usable on demand (timeliness) by an authorised entity."(Quelle: a.a.O. (Fn 24), Seite 9);

26 a.a.o. (Fn. 14), JC 2019 26, Seite 31, Annex B2, ICT security risk profile of an insurance and reinsurance undertaking.



Vertraulichkeit, die Integrität und die Verfügbarkeit von Informationen zu schützen. Auf dieser Grundlage sollen Unternehmen unter anderem verschiedene Sicherheitsmaßnahmen festlegen und einführen, wie etwa Sicherheitsüberwachungen und die Überprüfungen, Bewertungen und Tests der Informationssicherheit.

Im Rahmen der fast gleichlautenden Anforderungen an die Sicherheitsüberwachung sollen die Unternehmen ungewöhnliche Aktivitäten, die ihre Informationssicherheit beeinflussen können, identifizieren, kontinuierlich überwachen und erkennen. Sicherheitsrelevante Gefahren, die Unternehmen daran hindern, die Informationssicherheitsziele der Vertraulichkeit, Integrität und Verfügbarkeit ihrer IT-Assets zu schützen, sollen ebenso wie physisches oder logisches Eindringen erkannt und gemeldet werden. Hierfür sollen Unternehmen angemessene und effektive Funktionen einrichten.

Zur wirksamen Ermittlung von Schwachstellen in ihren IKT-Systemen und -Dienstleistungen sollen die Unternehmen regelmäßig und anlassbezogen Überprüfungen, Bewertungen und Tests in Bezug auf die Informationssicherheit durchführen. Hierzu sollen die Unternehmen ein entsprechendes Rahmenwerk entwickeln und implementieren sowie sicherstellen, dass die Tests von unabhängigen Prüfern durchgeführt werden. Die weiteren Ausführungen zu dieser Informationssicherheitsmaßnahme, beispielsweise zu detaillierten Testfrequenzen und zur Erfordernis einer Testumgebung für Zahlungsterminals und -geräte, sind alleinig in den EBA-Leitlinien aufgeführt und ergeben sich unter anderem aus dem Risikoprofil von Zahlungsdienstleistern und aus sektorspezifischen regulatorischen Vorgaben.

Die Leitlinien umfassen weiterhin Anforderungen zum Betriebs-, zum Projekt-, zum Änderungs- und zum Geschäftsfortführungsmanagement. Letztgenanntes beinhaltet eine Business-Impact-Analyse (BIA) und eine Geschäftsfortführungsplanung. Das Geschäftsfortführungsmanagement verpflichtet Unternehmen weitergehend, Reaktions- und Wiederherstellungspläne zu entwickeln, ihre Geschäftsfortführungspläne (BCPs) zu testen und eine wirksame Krisenkommunikation zu entwerfen. Bei der Geschäftsfortführungsplanung und beim Testen von Plänen zeigen sich im Detail Unterschiede bei den Anforderungen: Im Kontext der Geschäftsfortführungsplanung thematisiert die EBA Erfordernisse beim Umgang mit schwerwiegenden Betriebsunterbrechungen; im Zusammenhang mit dem Testen von Plänen geht sie detailliert auf zu erfüllende Anforderungen beim Testen der BCPs ein. Beide Aspekte berücksichtigt EIOPA aufgrund des spezifischen Risikoprofils von Versicherungsunternehmen insbesondere in Bezug auf das Informationssicherheitsziel der Verfügbarkeit beziehungsweise ihrer spezifischen regulatorischen Herangehensweise bei Erstellung von Leitlinien nicht.

Allgemein lässt sich festhalten, dass beide Leitlinien einem deutlichen Harmonisierungsansatz folgen, der sich aller Voraussicht nach auf Ebene europäischer Richtlinien fortsetzen wird. Bis zum Abschluss dieses europäischen Vorhabens tragen die beiden Leitlinien künftig wesentlich dazu bei, die Erwartungshaltung betreffend die Informationssicherheit der beiden europäischen Aufsichtsbehörden an die von ihnen beaufsichtigen Unternehmen darzustellen.

4 Harmonisierung regulatorischer Anforderungen zu Auslagerungen an Cloud-Service-Provider

Rahmenwerk zur Überwachung kritischer Dienstleister
Die ESAs haben eine gemeinsame Stellungnahme zur Auslagerung an Cloud-Anbieter veröffentlicht. Darin betonen sie, wie notwendig es sei, einen einheitlichen rechtlichen Rahmen für die Überwachung („oversight") kritischer Dienstleister zu schaffen.

Dieses Rahmenwerk soll einen Überblick über Risiken geben, die mit der Auslagerung (Outsourcing) an Drittparteien für die beaufsichtigten Unternehmen und den gesamten Finanzmarkt entstehen.

Ein Rechtsrahmen soll daher festlegen, wann eine Drittpartei als kritisch einzustufen ist. Dabei ist zu berücksichtigen, dass Drittparteien ihre Dienstleistungen grenzüberschreitend in und außerhalb der Europäischen Union anbieten. Aus diesem Grund favorisieren die Aufsichtsbehörden eine internationale Koordination.[27]

Dabei fokussieren die ESAs insbesondere Cloud Service Provider (CSPs) als Adressaten einer solchen Überwachung kritischer Dienstleister. In der aktuellen Situation bediene, so die ESAs, eine kleine Zahl an CSPs einen Großteil des Finanzmarkts. Ein Ausfall eines solchen Dienstleisters kann daher die Stabilität des gesamten Finanzsektors beeinflussen.

Die Harmonisierung und Kohärenz aufsichtlicher Anforderungen an die Informationssicherheit hat auch bei der Auslagerung an CSPs im Finanzsektor eine große Bedeutung. Dennoch besteht bei den beaufsichtigten Unternehmen eine gewisse Unsicherheit, wie sich aufsichtsrechtliche Vorgaben umsetzen lassen. Daher hat die EU-Kommission im FinTech-Aktionsplan die ESAs beauftragt zu prüfen, ob Leitlinien für die Auslagerung an CSPs erforderlich sind.

27 JC 2019 26, Seite 4, 18.

Die Ansätze der ESAs: Empfehlungen und Leitlinien
Auf europäischer Ebene standen EIOPA, EBA, der Einheitliche Aufsichtsmechanismus SSM (Single Supervisory Mechanism) und die nationalen Aufsichtsbehörden in den vergangenen Jahren im stetigen Austausch, was den Umgang mit Auslagerungen an Cloud-Anbieter betrifft. Im Jahr 2018 ist die EBA dem wachsenden Bedürfnis nach Orientierung begegnet: Als erste europäische Aufsichtsbehörde hat sie Empfehlungen zur Auslagerung an Cloud-Anbieter[28] veröffentlicht und damit einen wichtigen Schritt zu mehr Transparenz bei der Nutzung von Cloud-Diensten getan. EIOPA und ESMA folgen dieser europäischen Marschrichtung.

Im vergangenen Jahr hat die EBA diese Cloud-spezifischen Empfehlungen dann in ihre allgemeinen „Guidelines on outsourcing arrangements"[29] (siehe Infokasten) übertragen, weshalb die Empfehlungen zur Auslagerung an Cloud-Anbieter mit Wirkung zum 30. September 2019 aufgehoben wurden. Die anderen ESAs arbeiten indes weiter an ihren Cloud-spezifischen Handlungsempfehlungen.

So haben sich EIOPA und ESMA ein Beispiel an der EBA genommen. Im Februar hat EIOPA nach einer Konsultationsphase im vergangenen Jahr ihre „Guidelines on outsourcing to cloud service providers" veröffentlicht.[30] ESMA hat die Arbeit an solchen Leitlinien im vergangenen Jahr ebenfalls aufgenommen. Dabei haben EIOPA

28 EBA, Empfehlungen zu Auslagerung an Cloud-Anbieter, https://eba.europa.eu/sites/default/documents/files/documents/10180/2170125/afd89dc3-45a7-4054-a642-d03b4e35fa1f/Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03)_DE.pdf, abgerufen am 10.3.2020.

29 EBA, Leitlinien zu Auslagerungen, https://eba.europa.eu/sites/default/documents/files/documents/10180/2761380/5546a705-bff2-43eb-b382-e5c7bed3a2bc/EBA%20revised%20Guidelines%20on%20outsourcing_DE.pdf, abgerufen am 10.3.2020.

30 EIOPA, Leitlinien zum Outsourcing an Cloud-Anbieter, https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cor_de_0.pdf, abgerufen am 29.4.2020.

und ESMA aus Kohärenzgründen erklärt, nur dann vom Vorschlag der EBA abzuweichen, wenn dies aufgrund von Spezifika der jeweiligen Aufsichtsbereiche sinnvoll sein sollte.

Damit folgen die ESAs auch bei der Veröffentlichung der Leitlinien für Auslagerungen in die Cloud – wenn auch in individuellen Dokumenten – einem harmonisierten und kohärenten Regulierungsansatz. Das Ziel: Die europäische Aufsicht will Finanzunternehmen ihre Erwartungen transparent machen, um ihnen auf diese Weise die Umsetzung zu erleichtern.

Auf einen Blick

EBA Guidelines on Outsourcing arrangements

Die EBA-Guidelines sind am 30. September 2019 in Kraft getreten und haben die bis dahin geltenden Outsourcing Guidelines des EBA-Vorläufers CEBS[31] aus dem Jahr 2006 und die EBA-Empfehlungen zur Auslagerung an Cloud-Anbieter aus dem Jahr 2017 ersetzt. In diesen neuen Guidelines konkretisiert die EBA ihre Erwartungen an die Rahmenbedingungen für Auslagerungen. Darin betont die EU-Behörde insbesondere, dass das Leitungsorgan eines Unternehmens zu jeder Zeit für die eigenen Prozesse verantwortlich ist. Als großes Risiko identifiziert die EBA Auslagerungen in Drittstaaten. In diesem Fall müssen die Institute sicherstellen, dass etwa beim Datenschutz EU-Regularien eingehalten werden. In der Konsequenz betrifft dies auch mögliche Weiterverlagerungen.

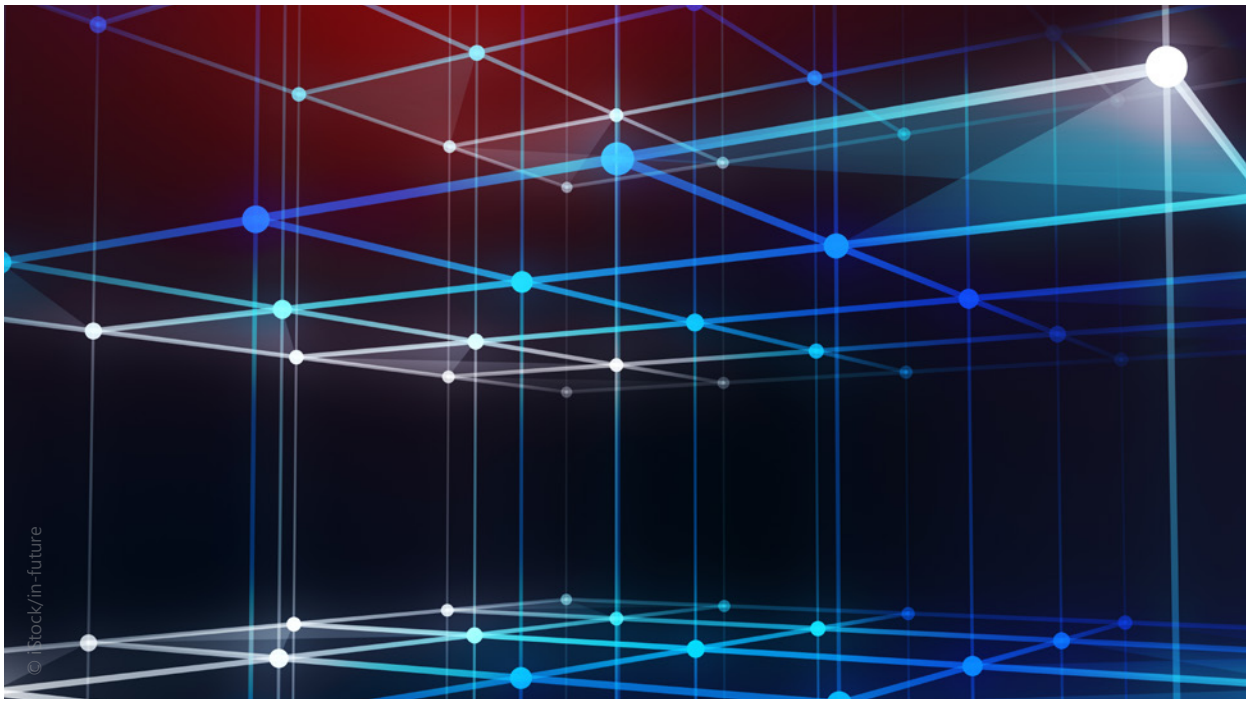
Die Guidelines bringen auch Neuerungen: So werden Institute beispielsweise verpflichtet, ein Register zu führen, das sämtliche Auslagerungen umfasst. Zudem müssen Institute die Aufsicht über neu geplante wesentliche Auslagerungen, materielle Veränderungen und schwere Vorfälle informieren. Auch sehen die Guidelines bei allen Auslagerungen Zugangs-, Informations- und Prüfrechte für Aufseher und Institute vor. Bei eher unwesentlichen Auslagerungen werden die Rechte jedoch nur risikobasiert verlangt. Finanzinstitute müssen diese Zugangs-, Informations- und Prüfrechte schriftlich in den Verträgen mit den Dienstleistern festhalten. Altverträge müssen sie den neuen Guidelines nach anpassen.

Ansatz der BaFin: Orientierungshilfe zu Auslagerungen an Cloud-Anbieter

Während EBA, EIOPA und ESMA sukzessive eigene Empfehlungen bzw. letztendlich Guidelines für Auslagerungen an Cloud-Anbieter veröffentlicht haben bzw. diese planen, hat die BaFin mit dem aufsichtsbereichsübergreifenden Merkblatt –„Orientierungshilfe zu Auslagerungen an Cloud-Anbieter" im November 2018 ein Dokument veröffentlicht, das dem europäischen Konzept der Harmonisierung und Kohärenz aufsichtlicher Anforderungen gerecht wird.[32] Denn das Merkblatt enthält Empfehlungen, die sich an die im Finanzsektor beaufsichtigten Unternehmen (Kreditinstitute, Finanzdienstleistungsinstitute, Versicherungsunternehmen, Pensionsfonds, Wertpapierdienstleistungsunternehmen, Kapitalverwaltungsgesellschaften, Zahlungsinstitute und E-Geld-Institute) richten und daher im Kontext der jeweils geltenden aufsichtsrechtlichen Anforderungen zu lesen sind. Diese haben die derzeitige aufsichtliche Praxis der BaFin und

31 Das Committee of European Banking Supervisors war Teil des Lamfalussy-Verfahrens der Europäischen Union.

32 Vgl. BaFinJournal April 2018, Seite 29 ff. und www.bafin.de/dok/11681122.



der Bundesbank in solchen Cloud-spezifischen Auslagerungsfällen im Fokus und sollen neben Hilfestellungen auch ein Bewusstsein für Probleme schaffen, die bei der Nutzung von Cloud-Diensten und den damit verbundenen aufsichtsrechtlichen Anforderungen auftreten können.

Im Fokus steht dabei neben der Erläuterung der Cloud-spezifischen Aspekte im Rahmen der Risikoanalyse insbesondere die Vertragsgestaltung. Die BaFin hat in der laufenden Aufsicht die Erfahrung gemacht, dass Finanzunternehmen vor allem die Vertragsgestaltung mit Dienstleistern erhebliche Schwierigkeiten bereitet hat. Auch Cloud-Anbieter, die ihre Dienstleistung schwerpunktmäßig anderen Branchen bieten, haben die aufsichtlichen Anforderungen eines stark regulierten Finanzmarktes zunächst vor Herausforderungen gestellt. An dieser Stelle hat zudem das BaFin-Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter" Klarheit geschaffen. Im Hinblick auf die Vereinbarung über uneingeschränkte Informations- und Prüfrechte der Aufsicht hat das BaFin-Merkblatt auch auf Seiten der Cloud-Anbieter Transparenz gebracht und so die Vertragsverhandlungen der beaufsichtigten Unternehmen zudem positiv beeinflusst.

Auch Hinweise, wie Prüfhandlungen leichter und effizienter gestaltet werden können, lassen sich dem BaFin-Merkblatt entnehmen. Zum Beispiel ist es möglich, Sammelprüfungen (Pooled Audits) abnehmen zu lassen. Dabei kann die interne Revision eines oder mehrerer auslagernder Finanzunternehmen, die unter Aufsicht der BaFin stehen, Informations- und Prüfrechte gegenüber dem Cloud-Anbieter wahrnehmen. Diese Erleichterung hat in der Finanzbranche bereits Zuspruch gefunden. Die Deutsche Börse etwa hat im Jahr 2017 die Collaborative Cloud Audit Group (CCAG) initiiert. Diese branchenweite Initiative, an der sich mehrere große europäische Finanzinstitute und Versicherungsgesellschaften beteiligen, hat bereits stellvertretend für ihre Mitglieder Prüfungen bei weltweit operierenden Cloud-Anbietern wie Microsoft durchgeführt.[33] Das ist ein Beleg dafür, dass die vertraglich geregelten Informations- und Prüfrechte der Finanzunternehmen in der Praxis durchgesetzt werden konnten.

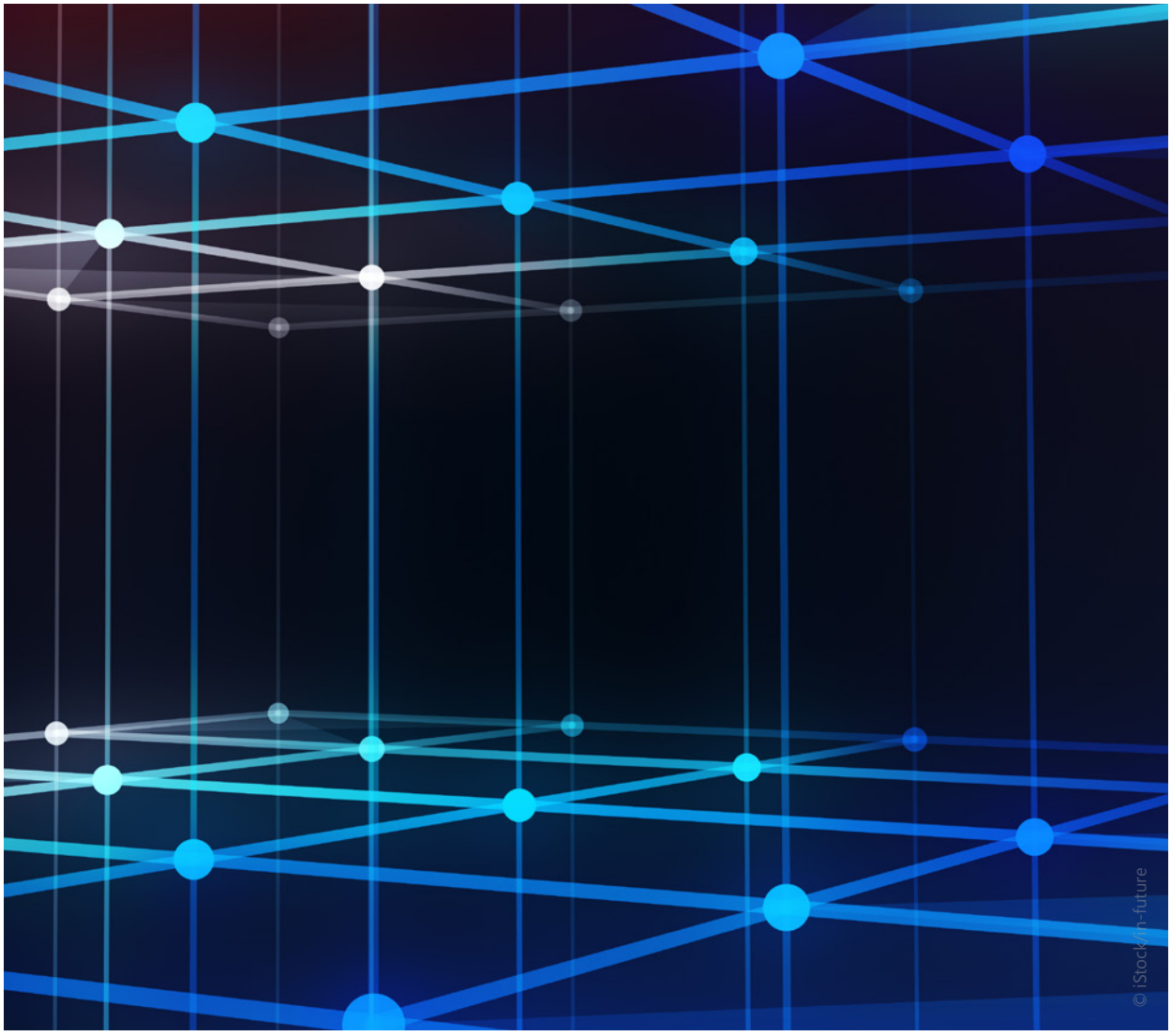
Die deutsche Finanzaufsicht strebt für den Bereich Cloud-Computing künftig noch weitere aufsichtliche Maßnahmen an. Der Grund: Die Sammelprüfungen bei Cloud-Anbietern haben gezeigt, dass vor allem Prüfungen in Drittstaaten die beaufsichtigten Finanzunternehmen fordern. Denn erhebliche personelle wie finanzielle Ressourcen sind dafür notwendig. Daher will sich die BaFin auf europäischer Ebene für neue regulatorische Standards einsetzen, um die Situation für die beaufsichtigten Unternehmen und die Finanzaufsicht zu erleichtern.

33 Pressemeldung Deutsche Börse Group, Deutsche Börse und Microsoft erreichen wichtigen Meilenstein für die Cloud-Nutzung im Finanzdienstleistungssektor https://www.deutsche-boerse.com/dbg-de/investor-relations/news-und-services/pressemitteilungen/Deutsche-B-rse-und-Microsoft-erreichen-wichtigen-Meilenstein-f-r-die-Cloud-Nutzung-im-Finanzdienstleistungssektor-1540064, abgerufen am 29.1.2020.

5 Fazit

Für die EU-Kommission, die europäischen Aufsichtsbehörden und die BaFin als nationale Finanzaufsicht ist die Harmonisierung und Konvergenz aufsichtlicher Anforderungen an die Informationssicherheit und das Cloud-Computing auf nationaler und europäischer Ebene von großer Bedeutung.

Die BaFin hat mit ihren Rundschreiben BAIT, VAIT, KAIT frühzeitig harmonisierte Anforderungen an die Informationssicherheit für weite Teile der Finanzbranche veröffentlicht ohne dabei sektorspezifische Aspekte außer Acht zu lassen. Im europäischen Kontext hat die deutsche Finanzaufsicht mit diesem Ansatz eine wegbereitende Rolle gespielt. Mit ihrem Merkblatt „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter" ist die BaFin noch einen Schritt weitergegangen – und hat einheitliche Anforderungen für alle beaufsichtigten Unternehmen formuliert. Mit ihren Veröffentlichungen trägt die BaFin damit der immer weiter zunehmenden Bedeutung der digitalen operationalen Resilienz und dem damit einhergehenden Harmonisierungs- und Regulierungsbedürfnis – auch im europäischen Kontext – Rechnung.



II

Cyber-Resilienz und Krisenmanagement – eine Aufgabe für Unternehmen und Aufsicht

Wie sich Deutschlands Banken gegen Cyberkriminalität rüsten

Autoren

Andreas Krautscheid
Hauptgeschäftsführer,
Bundesverband deutscher Banken

André Nash
Abteilungsdirektor,
Themengruppe Banktechnologie und Sicherheit,
Bundesverband deutscher Banken

1 Einleitung

Die Coronakrise hat uns wieder einmal vor Augen geführt, welche Schlüsselfunktion Banken ausüben und dass sie eine zentrale Verantwortung in der Volkwirtschaft haben. Das Bankgeschäft muss funktionieren; Beeinträchtigungen oder gar massive Störungen müssen unter allen Umständen verhindert werden.

In den vergangenen Jahren hat die Gefahr von Cyberattacken auf Deutschlands Wirtschaft und damit auch auf den Finanzsektor erheblich zugenommen. Die beiden wesentlichen Gründe hierfür liegen auf der Hand: zum einen die digitale Transformation sämtlicher Bereiche unseres Gesellschafts- und Wirtschaftslebens sowie eine stärkere Vernetzung der Unternehmen, durch die beständig neue Einfallstore für Angreifer geschaffen werden; zum anderen die zunehmende Professionalisierung der Cyberkriminellen, die ihr technologisches Waffenarsenal kontinuierlich aufrüsten. Nicht ohne Grund werden Cyberangriffe gegenwärtig als das größte operationelle Risiko im Finanzsektor gesehen.

Schon heute sind die digitalen Systeme vieler Unternehmen, nicht zuletzt der Kreditinstitute, so komplex, dass es schlicht unmöglich ist, generell jeden Angriff zu verhindern. Hinzu kommt, dass Fortschritte im Bereich künstliche Intelligenz (KI) neue und perfektionierte Attacken ermöglichen. So wurden im vergangenen Jahr verstärkt Fälle von Telefonbetrug registriert, bei denen die Täter mit Hilfe von KI Stimmen manipulierten und so den Versuch unternahmen, Mitarbeiter von Unternehmen zu täuschen und Gelder zu ergaunern. Für 2020 wird mit einem deutlich höheren Einsatz solcher Deepfakes gerechnet, zu denen auch gefälschte Videos zählen. Hier wird auf KI zurückgegriffen, um dynamisch Daten zu verändern. Angriffe autonom durchführen werden diese Systeme jedoch vorerst nicht. Denn noch bedarf es zu einem wesentlichen Teil der menschlichen Intelligenz, um Sicherheitslücken zu finden, Angriffsszenarien zu entwerfen und Attacken tatsächlich durchzuführen.

Während die aktive Ausnutzung von Sicherheitslücken also vorerst eine menschliche Domäne bleibt, ist das Aufspüren von Bugs[1] und deren Beseitigung eine Stärke autonomer, auf KI basierender Systeme. In welche Richtung die Entwicklung gehen kann, zeigt ein reales Beispiel: Auf einer DARPA[2]-Hacker-Konferenz fand ein System in einer vorab präparierten Testumgebung einen Bug, von dem der Veranstalter nichts wusste, und startete eine erfolgreiche Attacke gegen ein anderes System. Ein drittes System hat dies beobachtet, den Angriff „reverse engineered", den Bug gefunden, einen Patch[3] geschrieben und bei sich selbst installiert – alles innerhalb von 20 Minuten. So sieht die Realität heute noch nicht überall aus, aber es wird deutlich, wohin sich solche Ansätze künftig entwickeln werden.

Daneben gibt es noch einen weiteren potenziellen Risikoherd: Die Banken haben IT-Systeme zunehmend auf eine vergleichsweise kleine Zahl von IT-Dienstleistern verlagert und nehmen obendrein verstärkt Cloud-Dienstleistungen in Anspruch. Ein Ausfall oder die eingeschränkte Verfügbarkeit eines Dienstleisters durch einen Cyberangriff könnte daher erhebliche Auswirkungen haben. Um beim Beispiel Cloud zu bleiben: Die Vorteile und Potenziale einer Einbindung von Cloud-Lösungen in die Bankprozesse und -systeme liegen auf der Hand. Da die Angebotsseite – mit gerade einmal einer Handvoll relevanter, globaler Cloud-Dienstleister – recht übersichtlich ist, droht hier jedoch eine hohe Konzentration vieler Banksysteme auf wenige Cloudsysteme. Und trotz der Fähigkeit der einzelnen Cloudsysteme, über eine Netzwerkarchitektur die Ausfallrisiken so stark zu streuen, dass Ausfälle fast unmöglich sind, können Einschränkungen in der Praxis doch auftreten. So waren im Sommer 2019 beispielsweise mehrere Google-Dienste, die über die Cloud des Internetkonzerns betrieben werden, zeitweise ausgefallen. In Summe drohen nicht nur finanzielle oder Reputationsschäden für die einzelne Bank, sondern auch systemische Schäden für den gesamten Finanzsektor. Aus diesem Grund ist das gesamte System gefordert, die Bedrohungslage laufend zu analysieren und Maßnahmen koordiniert zu ergreifen.

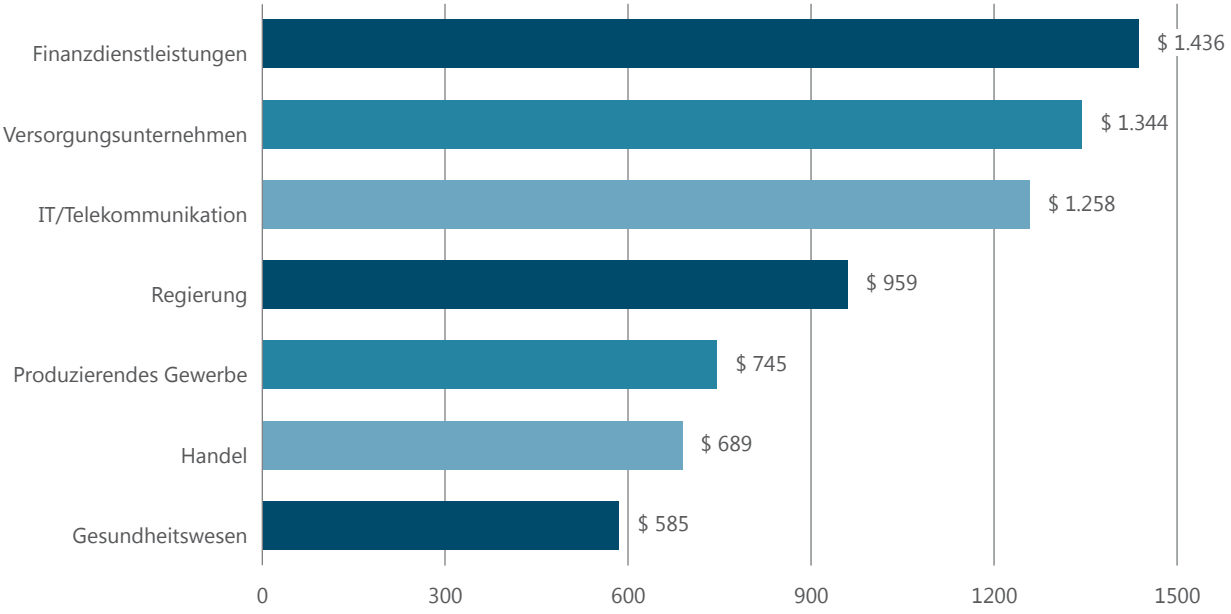
1 Softwarefehler oder Software-Anomalien, die zu einem Fehlverhalten von Computerprogrammen bzw. zu Sicherheitslücken führen können.
2 DARPA bedeutet Defense Advanced Research Projects Agency. Die DARPA ist eine Behörde des Verteidigungsministeriums der USA, die Forschungsprojekte für die Streitkräfte der Vereinigten Staaten umsetzt.
3 Korrekturauslieferung für Software, um Fehler zu beheben, bekannt gewordene Sicherheitslücken zu schließen oder bislang nicht vorhandene Funktionen nachzurüsten.

2 Gewachsene Expertise – Banken sind von Stunde null an dabei

Cyberrisiken sind für die gesamte Kreditwirtschaft eine ernstzunehmende Herausforderung. Aber: Kreditinstitute verfügen auch über eine besondere Expertise zum Schutz ihrer technischen Infrastrukturen. Seit Beginn des Online-Bankings im November 1980 – also seit fast 40 Jahren – stellen Cyberangriffe ein relevantes Thema für unsere Mitgliedsinstitute dar. Die kontinuierliche Weiterentwicklung der Sicherheitssysteme zum Schutz der Kundendaten und des Kundenvertrauens genießen schon seit langer Zeit höchste Priorität bei den Banken. Dies spiegelt sich auch in den Investitionen wider, die in diesem Bereich getätigt werden. Einer weltweiten Umfrage des Cybersicherheitsunternehmens Kaspersky zufolge sind Banken bei den Investitionen in Cybersicherheit pro Mitarbeiter führend.[4]

4 Kaspersky Lab Security Economics Report, Seite 12.

Abbildung 1: Ausgaben für Cybersicherheit pro Mitarbeiter



Quelle: Kaspersky Lab Corporate IT Security Risks Survey

3 Unsicherheitsfaktor Mensch

Das sicherste technische System kann allerdings keinen ausreichenden Schutz bieten, wenn die Nutzer dieses Systems die grundlegenden Sicherheitsanforderungen nicht beachten. Denn das vielleicht größte Einfallstor für Cyberattacken ist der Mensch selbst. Angriffspunkte sind Einzelpersonen, über deren Zugangsdaten Cyberkriminelle versuchen, Zugriff auf Konten oder Banksysteme zu bekommen. Das Spektrum der Attacken reicht von breit gestreuten Phishing[5]-E-Mails bis hin zu gezielten Angriffen auf einzelne, speziell ausgewählte Personen, die teilweise über viele Monate ausspioniert werden (Spear-Phishing-Angriffe). Banken betreiben deshalb zurecht einen hohen Aufwand für Schulungen, Awareness-Kampagnen und Aufklärungsarbeit, um Mitarbeiter und Kunden kontinuierlich zu informieren und zu sensibilisieren.

5 Als Phishing bezeichnet man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen.

4 Bedeutung von Informationsaustausch und Netzwerken steigt

Inzwischen ist die unternehmens- und sektorübergreifende Vernetzung der Cybersicherheitsverantwortlichen genauso wichtig wie ihre IT-Kompetenz. Das Information Sharing ist ein wesentliches Instrument bei der Abwehr und Bekämpfung von Cyberangriffen. Eine kurzfristige Benachrichtigung der Community bei einem aktuell stattfindenden Angriff versetzt die Branche in Alarmbereitschaft und ermöglicht, dass die Abwehrsysteme sehr schnell auf die konkreten Angriffsvektoren eingestellt werden können. Und auch der Austausch über ausgewertete Vorfälle ist für die Banken unerlässlich, um den bestmöglichen Schutz sicherzustellen. Schadsoftware kann manchmal wochen- oder monatelang vor anderen verborgen werden. Ein möglicher Schaden tritt dann auf, wenn diese Software aktiv und der Angriff durchgeführt wird – dann schlagen die Abwehrsysteme an. Kann diese Software jedoch im Vorfeld durch Systemanalysen – aufgrund von ausgetauschten Informationen – identifiziert werden, hilft dies bei der Abwehr und auch bei der Prognose weiterer möglicher Angriffsszenarien. Darüber hinaus leisten diese Informationen einen erheblichen Beitrag für die Prävention weiterer Angriffe, indem sie Teil der ständigen Weiterbildung von Mitarbeitern und IT-Sicherheitsexperten werden. Und auch für die Strafverfolgung von Angreifern sind die zu den Attacken gesammelten Daten relevant, denn nicht selten führen sie zur Ergreifung von Cyberkriminellen.

Der freiwillige, regelmäßige Austausch von Informationen zwischen Banken, Sicherheits- und Strafverfolgungsbehörden reicht allein jedoch nicht aus. Auf verschiedenen Plattformen werden heute zahlreiche Informationen zu aktuellen Angriffen, neuer Schadsoftware und laufenden Phishing-Kampagnen oftmals ungefiltert ausgegeben. Aufgrund der enormen Menge weltweiter Cyberaktivitäten ist die Masse dieser Rohdaten allerdings so

groß, dass dies ihren Nutzen zugleich in Frage stellt. Denn bevor Informationen in die Abwehrsysteme einer Bank einfließen können, müssen der Angriff analysiert und die notwendigen Abwehrmaßnahmen mit Blick auf die eigenen Systeme bewertet werden, um neue Risiken durch Systemanpassungen zu vermeiden. Daher besteht Bedarf an besser gefilterten und bereits ausgewerteten Informationen, die für die eigenen Systeme relevant sind – und das so zeitnah wie möglich.

Es gibt ein weiteres Problem: Leider führt die zunehmend unübersichtliche IT-Sicherheitsregulierung im Finanzsektor zu Unsicherheiten darüber, welche Informationen (noch) mit wem geteilt werden dürfen. Um die Möglichkeiten insbesondere auch für einen grenzüberschreitenden Austausch zu verbessern, wäre es hilfreich, Inkonsistenzen und Interpretationsspielräume – insbesondere, wenn es sich um personenbezogene Daten handelt, – zu adressieren. Aus diesem Grund bemüht sich die Finanzdienstleistungsbranche um Rechtssicherheit hinsichtlich der Möglichkeiten für Finanzinstitute, Informationen über Betrugsbedrohungen innerhalb der Branche auszutauschen. Hier brauchen wir EU-weit einheitliche Rahmenbedingungen, die ausdrücklich den Austausch bestimmter Informationen und Erkenntnisse zwischen privaten Einrichtungen sowie zwischen dem privaten und dem öffentlichen Sektor erlauben. Generell gilt: Die Verflechtung der staatlichen und der privatwirtschaftlichen Sicherheitsereignis- und Reaktionsteams in den Unternehmen mit den (Sicherheits-)Behörden ist eine wesentliche Voraussetzung, um mögliche Großereignisse bewältigen zu können. Ereignisfeststellung, -bewertung und gegebenenfalls die Krisenreaktion sind in der Cybersicherheit eine Gemeinschaftsaufgabe und müssen auch als solche bewältigt werden.

5 Regulierungsmaßnahmen müssen harmonisiert werden

Die zunehmenden Cyberangriffe auf Banken sind in den vergangenen Jahren auch zu einem immer wichtigeren Thema für die Aufsichtsbehörden geworden, da sie die Stabilität des Finanzsektors gefährden können. Auf europäischer Ebene haben die Europäische Zentralbank (EZB) und die Europäische Bankenaufsicht (EBA) inzwischen ihre jeweiligen Vorstellungen zur Erhöhung der Cyberwiderstandsfähigkeit des Finanzsektors konkretisiert. Und auf EU-Ebene haben Europäischer Rat und Europäisches Parlament unter anderem die Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie), die Zweite Zahlungsdiensterichtlinie (PSD2) und den Cyber Security Act beschlossen.

Grundsätzlich decken sich die Anforderungen der Aufsicht mit den Bestrebungen und Aktivitäten der Banken. Allerdings sind die Regulierungsvorgaben der einzelnen Aufsichtsbehörden oftmals nicht aufeinander abgestimmt. Die Folge: Der Aufwand, den die Kreditinstitute zu erbringen haben, ist enorm. Banken müssen gegenüber jeder einzelnen Behörde nachweisen, dass sie die Anforderungen erfüllt haben; obendrein müssen sie umfangreiche Fragenkataloge beantworten und denselben Vorfall auf unterschiedlichen Formularen an mehrere Meldestellen senden. Dass dies nicht sinnvoll sein kann, liegt auf der Hand. Es wäre sehr viel effizienter, die hierfür notwendigen Ressourcen direkt in die Verteidigungssysteme zu stecken. Eine Harmonisierung der Vorgaben und eine organisierte Meldestruktur für die Nachweiserbringung und das Reporting sind daher zwingend erforderlich. Sie würden zu einem insgesamt höheren Sicherheitsniveau, zu angemessenen Aufsichtspraktiken und zugleich zu einem niedrigeren Verwaltungsaufwand führen. Die aktuelle öffentliche Konsultation der Europäischen Kommission zur Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen[6] zeigt, dass diese Notwendigkeit von Aufsicht und Politik erkannt wird. Nur: Was folgt daraus? Es wäre keine gute Nachricht, wenn als Ergebnis zwar neue Regulierung auf die Banken zukäme, die notwendige Komplexitätsreduzierung aber ausbliebe.

Harmonisierung ist im Übrigen auch bei den Threat Intelligence-based Ethical Red Teamings, den TIBER--Tests, ein wichtiges Thema. Diese simulierten Hacker-Angriffe basieren auf einem Rahmenwerk der EZB: Während die EZB sich auf die Finanzmarktinfrastrukturen fokussiert, setzen die nationalen Zentralbanken und Aufsichtsbehörden diesen Testansatz für die jeweiligen Banken in den einzelnen Mitgliedstaaten um. Hier sehen wir derzeit allerdings noch zahlreiche ungeklärte Aspekte, beispielsweise hinsichtlich einer möglichen Zertifizierung der testenden Unternehmen (Red-Teams) oder der Vergleichbarkeit der jeweiligen nationalen Tests. Im Sinne des angestrebten harmonisierten Ansatzes wäre es wichtig, dass ein in einem Land durchgeführter Test durch die anderen EU-Mitgliedstaaten anerkannt wird, um doppelte Tests und unnötige Mehraufwendungen zu vermeiden. Darüber hinaus ist für die global agierenden Häuser wichtig, dass eine Vergleichbarkeit – bestenfalls Anerkennung – von TIBER mit den jeweiligen Test-Ansätzen außereuropäischer Länder gewährleistet wird, zum Beispiel mit dem CBEST-Rahmenwerk der Bank of England.

6 Europäische Kommission, Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf, abgerufen am 27.4.2020.

6 Technischer Wettlauf erfordert nationale und internationale Zusammenarbeit

Es ist absehbar, dass die Banken im Jahr 2020 mit deutlich raffinierteren und womöglich größeren Cyberangriffen rechnen müssen als in der Vergangenheit. Da sich die Täter technologisch weiterentwickeln und inzwischen in etwa das Niveau der nationalen Sicherheitsbehörden erreicht haben, müssen alle Kräfte gebündelt werden. Nur wenn Wissen geteilt und Innovationen gefördert werden, wird es gelingen, den Kriminellen einen Schritt voraus zu sein. Dabei darf der globale Aspekt nicht vernachlässigt werden. Cyberangriffe auf Banken können von überall auf der Welt aus gestartet werden – und globale Auswirkungen auf das Finanzsystem haben. Der einzig sinnvolle Weg ist daher eine international koordinierte Vorgehensweise. Banken, Sicherheitsindustrie sowie die relevanten nationalen und supranationalen Behörden müssen an einem Strang ziehen.

Lösungen für Probleme, die es noch gar nicht gibt

Autor

Professor Dr. Igor Podebrad
Bereichsvorstand Cyber Risk & Information Security und Group Chief Information Security Officer, Commerzbank AG

1 Cyber-Resilienz als zentraler Bestandteil der Sicherheitsstrategie

Der Trojaner Emotet[1] richtet noch immer großen Schaden in weiten Teilen der Wirtschaft an. Infiziert das weltweit gefährliche Schadprogramm das IT-System eines Unternehmens, lädt es weitere schädliche Software. Daten fließen ab, und kriminelle Hacker können die vollständige Kontrolle über das gesamte System erlangen.

In einer Vielzahl von Unternehmen und öffentlichen Einrichtungen wie Krankenhäusern fiel die IT-Infrastruktur schon großflächig oder komplett aus. In der Industrie waren mehrtägige Produktionsausfälle die Folge. Das Berliner Kammergericht beispielsweise ist wegen solch eines Schadsoftware-Befalls seit September 2019 offline und kann immer noch nicht wieder voll digital arbeiten.[2]

Europäische Banken wiederum konnten größere Schäden bislang erfolgreich abwenden. Emotet hat nur sehr vereinzelte Institute ernsthaft getroffen – zumindest noch.

Doch diese Schadsoftware zeigt uns anschaulich, dass wir in Banken und weiteren Finanzunternehmen nicht allein auf Prävention setzen dürfen.

Aufgrund der fortschreitenden Professionalisierung von Cyberangriffen können größere Sicherheitsvorfälle nie vollständig ausgeschlossen werden. Zwar kann und muss das Risiko durch technische Maßnahmen und erhöhtes Bewusstsein der Mitarbeiter stark reduziert werden, doch dadurch allein sind solche Vorfälle nicht vermeidbar.

Denn irgendwann wird eine Mail mit Schadsoftware nicht von Spam- und Virenscannern erkannt, und irgendwann klickt ein Mitarbeiter trotz Awareness-Training in der Mail auf den Link, der die Schadsoftware aktiviert. Bei solch einer akuten Cyberattacke muss eine vorausschauende Sicherheitsarchitektur den möglichen Schaden eindämmen: Die Infektion muss schnellstens detektiert, erkannt und die Verbreitung gestoppt werden, um dann mit der Wiederherstellung der Daten zu beginnen.

Entscheidend ist also, das Finanzunternehmen so auszurichten, dass es auch in einem Störfall gut gesteuert werden kann und, wenn überhaupt, nur minimal an Betriebsfähigkeit einbüßt.

1 vgl. zu Emotet auch Seite 13 ff. und 17.

2 vgl. u.a. Berliner Morgenpost, Cyberangriff auf Berliner Kammergericht: Ein Protokoll, https://www.morgenpost.de/berlin/article228301127/Cyberangriff-auf-Berliner-Kammergericht-Ein-Protokoll.html, abgerufen am 17.4.2020. Anm. d. Redaktion: Bis zum Redaktionsschluss konnte das Berliner Kammergericht immer noch nicht voll digital arbeiten.

2 Cyberrisiken müssen genauso gemanagt werden wie alle anderen wesentlichen Risikoarten

Cyber-Resilienz, also die Widerstandsfähigkeit eines Betriebs, ist ein zentraler Bestandteil der Sicherheitsstrategie von Banken. Verantwortlich dafür ist der Chief Information Security Officer, CISO. Seine Aufgabe ist es, in Zeiten von Cyberrisiken, Fake News und Corona-Pandemie die Balance zwischen Produktionsstabilität und den zusätzlichen Anforderungen an die Informationssicherheit herzustellen.

Das erfordert ein grundlegendes Umdenken im Management. Denn von vornherein muss immer auch die Möglichkeit eines schwerwiegenden Cybervorfalls oder einer Störung mitgedacht werden. Dafür reicht der punktuelle Blick auf technische Systeme nicht.

Im Fokus steht dabei, wie das Unternehmen überhaupt mit unvorhergesehenen Störungen umgeht. Es müssen Geschäftsprozesse, ganze Geschäftsbereiche, die Organisation sowie die Unternehmensführung und -kultur aus diesem Blickwinkel betrachtet und darauf ausgerichtet werden.

Hinzu kommt, dass auch die Bankenaufsicht der BaFin darauf großen Wert legt, was sich inzwischen in der Aufsichtspraxis niederschlägt. Aufseher und Regulierer erwarten, dass Finanzunternehmen Cyberrisiken genauso managen wie alle anderen wesentlichen Risikoarten.

Der Grund: Cyberrisiken sind Querschnittsrisiken und haben hochgradigen Einfluss auf die gesamte Risikolage der Bank. Demnach sollten Cyberrisiken mit ihrem operativen, technischen, finanziellen und reputationsrelevanten Bedrohungspotenzial mit allen anderen Risikoarten der Bank stringent und konsequent betrachtet und abgebildet werden.

Die Position des CISO, des obersten Sicherheitsbeauftragten, ist daher inhaltlich und organisatorisch idealerweise beim Risikovorstand des Konzerns angesiedelt. Denn im Zweifelsfall muss er bei einem Cyberangriff sehr schnell reagieren. Oft auch anders als ursprünglich geplant, denn Cyberangriffe sind dynamisch und detaillierte Maßnahmen schwer im Voraus zu planen.

Agilität ist daher elementar für die Cyber-Resilienz einer Organisation. Dafür benötigt der CISO ausreichende Informationen, um angemessen kontrollieren und steuern zu können. Zur Widerstandsfähigkeit gehört aber auch, dass Software-Tests und -Betriebsverfahren weitgehend automatisiert und integriert werden.

3 Die Cyber-Resilienz der Kunden spielt in die Risikobewertung hinein

Cyberrisiken sind schwer zu prognostizieren und deshalb schwer zu modellieren. Im Vergleich zu den etablierten Risikodaten gibt es nur wenige historische, statistisch valide Daten. Zudem ist die Eintrittswahrscheinlichkeit sehr gering, während der potenzielle Schaden sehr hoch ist.

Hinzu kommt der enorme Modernisierungs- und Wettbewerbsdruck, dem Banken aktuell ausgesetzt sind. Institute müssen sehr schnell auf Marktveränderungen reagieren und Produkte einführen, die noch nicht vollständig ausgereift sind. Time-to-market[3] ist nun einmal das Gebot in der digitalen Welt. Um diesem Lieferdruck gerecht zu werden, ist man heute eher bereit, ein gewisses Fehlerrisiko zu akzeptieren. Aus Sicherheitsaspekten stellt das natürlich eine Herausforderung dar. Denn diese Fehler können Angriffe ermöglichen, die mit anderen Prozessen mitigiert werden müssen.

Die Cybersicherheitsstrategie einer Bank bezieht auch sämtliche Prozesse beim Kunden ein. Lieferketten von Geschäftspartnern sollten hinsichtlich ihrer Sicherheit und Resilienz transparent und prüfbar sein.

Unsere Kunden können von dieser Kompetenz profitieren. Indem wir als Commerzbank ihr Bewusstsein für diese Themen schärfen, tragen wir zu ihrer und unserer Sicherheit bei. Auch die Cyber-Resilienz der Kunden spielt bis in die Risikobewertung der Bank hinein.

Ein Beispiel hierfür ist die CEO-Fraud. Dabei handelt es sich um eine Betrugsmasche, bei der sich ein Krimineller gegenüber einem Mitarbeiter per E-Mail oder Telefon als Unternehmenschef ausgibt und ihn zu einer betrügerischen Zahlung verleitet: Eine vertrauensvolle und wertschätzende Unternehmenskultur führt eher dazu, dass ein leicht verunsicherter Mitarbeiter sich von Mensch zu Mensch beim vermeintlichen Auftraggeber über die Authentizität des Auftrags vergewissert.

3 Time-to-Market ist die Zeitspanne, die von der Idee für ein Produkt bis zu dessen Markteinführung reicht.

4 Es darf keinen Wildwuchs in der Cyberregulierung geben

Die Online-Durchdringung der Wirtschaft und Gesellschaft hat inzwischen eine Dimension erreicht, die eine staatliche Regulierung unumgänglich macht.

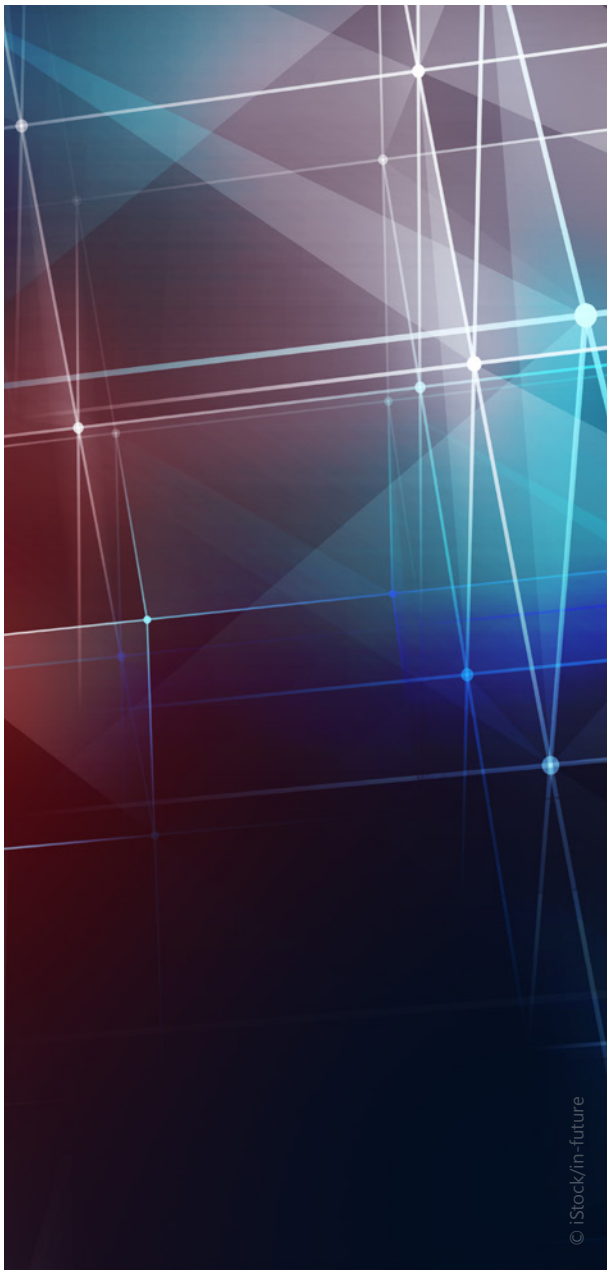
Regulierung ist wichtig und richtig. Doch die Zahl von Cybersicherheitsregeln wächst unaufhörlich. Für Unternehmen wird es zunehmend aufwändiger, die Flut von im Kern zumeist ähnlichen Regeln einzuhalten: Widersprüche zwischen Datenschutz- und IT-Sicherheitsrecht, Ungereimtheiten zwischen sektoralen und branchenübergreifenden Regeln, Inkompatibilitäten zwischen nationalen Regelungen, Doppelregulierungen und vielfache Meldeprozesse an verschiedene Behörden für einen einzigen Vorfall, weil jedes Formular ein wenig anders ist.

Da Cyberattacken nicht nur innerhalb der heimischen Landesgrenzen ausgelöst werden, brauchen wir international einheitliche Regeln (Level Playing Field).

Mit dem Cyber-Security-Rahmenwerk Tiber-EU[4] der Europäischen Zentralbank (EZB) wird über innereuropäische Grenzen hinweg höhere Cyber-Resilienz für Finanzinstitute angestrebt. Die EZB definiert in diesem Rahmenwerk ein Vorgehen, um die Verteidigungsfähigkeit eines Instituts durch einen kontrollierten Cyberangriff herauszufordern.

So klopfen die beauftragten Red Teams nicht nur die technischen Schwachstellen ab, sondern testen auch menschliche Faktoren mithilfe von Social-Engineering-Angriffen. Diese Tests sind sehr aufwändig und laufen über viele Monate. Auch außereuropäische Jurisdiktionen setzen auf Red-Teaming in ihren kritischen Infrastrukturen. Hier ist eine gegenseitige Anerkennung als genormter Test nötig.

Allerdings darf es keinen Wildwuchs in der Cyberregulierung geben. Die Eckpunkte liegen auf der Hand: transparentes Risikomanagement, Sicherheitsmaßnahmen nach dem Stand der Technik, Meldung von Vorfällen, Zusammenarbeit von Staat und Wirtschaft. Gesetzgeber, Wissenschaftler und Unternehmen sind gefordert, ein transatlantisches Rahmenwerk zu erarbeiten, das als Fundament für Cybersicherheit in Europa und den USA dienen kann – und als Vorbild für die Welt.



4 vgl. dazu auch Seite 47 ff.

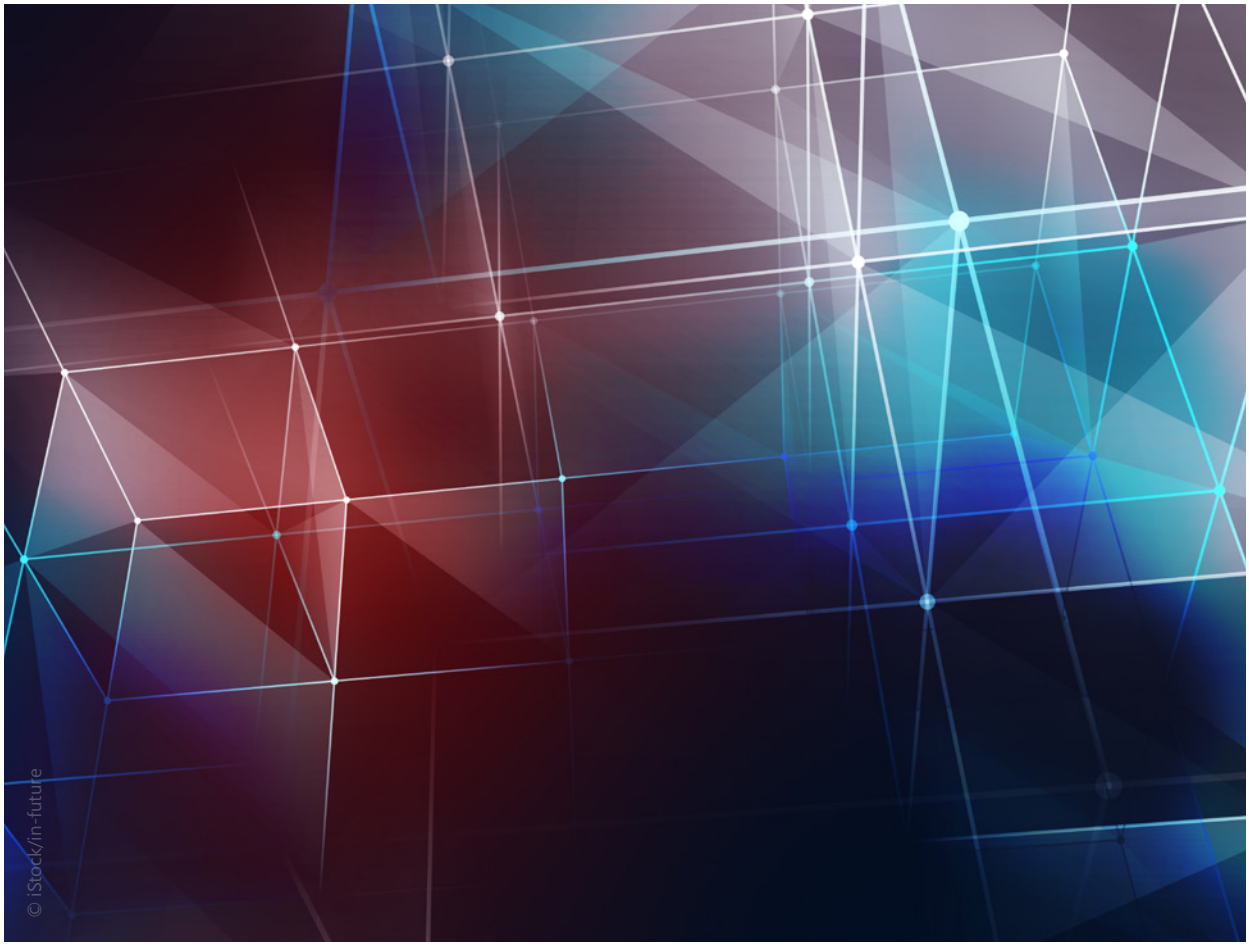
5 Neue Technologien bedrohen die Cybersicherheit

Der Durchbruch von neuen Technologien wie Biometrie, künstliche Intelligenz und Quantencomputer ist teils geschehen oder steht kurz bevor. Mit den neuen technologischen Möglichkeiten entstehen aber auch neue Formen der Bedrohung für die Cybersicherheit.

Denn Quantum Computing[5] hat beispielsweise hat das Potenzial, weitverbreitete Sicherheitsverfahren außer Kraft zu setzen. Deshalb treffen wir bereits heute Entscheidungen, um sicherzustellen, dass man dieser Gefahr in der Zukunft adäquat begegnen kann.

Mit diesem vorrausschauenden Ansatz stößt man intern nicht immer auf Gegenliebe und Verständnis. Warum sollte sich ein Unternehmen mit Lösungen präparieren, für die es noch keine Probleme gibt? Weil die Zukunft meistens schon da ist, bevor wir damit rechnen.

5 Quantum Computing bezeichnet das Arbeiten mit Quantencomputern. Deren Konstruktionsweise basiert auf der gezielten Nutzung quantenmechanischer Effekte für die Speicherung und Verarbeitung von Daten.



Cyber-Resilienz mittels TIBER-DE – Ein zukünftiges Rahmenwerk für ethische Hackerangriffe auf Finanzunternehmen in Deutschland

Autoren

Silke Brüggemann
Referat Grundsatz, IT-Aufsicht und Prüfungswesen, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Dr. Miriam Sinn
Leiterin TIBER Cyber Team Deutschland, Deutsche Bundesbank

Christoph Ruckert
Referat Grundsatz, IT-Aufsicht und Prüfungswesen, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

1 Einleitung

Die zunehmende Digitalisierung im Finanzsektor und die Gefahr von Cyberangriffen auf Banken, Versicherungen und Finanzmarktinfrastrukturen rücken die Widerstandsfähigkeit der Unternehmen als auch ihrer wichtigsten Dienstleister gegen interne wie externe Attacken immer stärker in den Fokus.

Die Europäische Zentralbank (EZB) hat im Mai 2018 daher das sektor- und unternehmens-unabhängige Rahmenwerk TIBER-EU (TIBER: Threat Intelligence-based Ethical Red Teaming) veröffentlicht. Die Ziele sind, eine angemessene Cyber-Resilienz (siehe Infokasten, Seite 48) der Unternehmen als wesentlichen Faktor für ein funktionsfähiges, stabiles und integres Finanzsystem zu fördern und die Vergleichbarkeit wie auch gegenseitige Anerkennung der Ergebnisse solcher Penetrationstests im europäischen Rahmen zu ermöglichen.

TIBER-Tests stellen ein geeignetes Instrument dar, die Cyber-Resilienz von Unternehmen mit einem hohen Reifegrad der Informationssicherheit weiter zu erhöhen. Bei solch einem Test werden simulierte Angriffe von externen, sogenannten ethischen Hackern auf ein Unternehmen durchgeführt. Ziel ist, die Präventions-, Detektions- und Reaktionsfähigkeiten des Unternehmens gegen Cyberangriffe auf ihre Wirksamkeit hin zu prüfen, indem vorab erhobene Informationen über die Bedrohungssituation des Unternehmens genutzt und

Instrumente professioneller Angreifer verwendet werden. Dabei stehen explizit für die Leistungserbringung kritische Prozesse des Unternehmens im Fokus. Im Gegensatz zu klassischen Penetrationstests zielen TIBER-Tests nicht alleine auf technische Schwachstellen ab, sondern beziehen auch den Faktor Mensch in die Angriffsszenarien ein.

Definition

Cyber-Resilienz

Cyber-Resilienz bezeichnet die Widerstandsfähigkeit von Unternehmen gegen Angriffe auf die Sicherheit ihrer Informations- und Kommunikationstechnik (IKT). Im Fokus der Angreifer stehen die Systeme der Unternehmen oder auch die Daten von Kunden. [1]

1 Vgl. BaFinJournal April 2019, Seite 26 ff. und BaFinJournal September 2019, Seite 8 ff.

2 Implementierungen in anderen Ländern

Das TIBER-EU-Rahmenwerk ist bisher in Belgien, Dänemark, Irland und in den Niederlanden umgesetzt worden.[2] Das niederländische Rahmenwerk TIBER-NL[3] war die erste nationale Implementierung und diente in vielerlei Hinsicht als Inspiration für andere nationale Programme.[4] Weitere Länder haben eine Implementierung angekündigt beziehungsweise arbeiten an konkreten Schritten zur Umsetzung.

Die ersten Erfahrungen mit TIBER-Tests aus den Niederlanden zeigen, dass TIBER ein erfolgsversprechendes Konzept für die Durchführung von bedrohungsgeleiteten Penetrationstests ist. Anfangs beschränkte sich die Zielgruppe auf Finanzinstitutionen und deren kritische Infrastruktur, wurde aber inzwischen auf Versicherungsunternehmen und Pensionsfonds ausgeweitet. Sogar ein erstes Pilotprojekt im Energiesektor gab es in den Niederlanden bereits.[5]

Eine weitere positive Entwicklung in den Niederlanden ist die Entstehung von TIBER-Netzwerken, über die sich Unternehmen verknüpfen, die an einem TIBER-Test teilgenommen haben. Diese Netzwerke tragen dazu bei, notwendiges Vertrauen und die Kooperation in der Industrie auf dem Gebiet der TIBER-Tests aufzubauen. Ziel der deutschen Umsetzung ist es, auch in dieser Hinsicht von den Erfahrungen in anderen Ländern zu lernen.

Die Deutsche Bundesbank und die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) entwickeln TIBER-DE basierend auf dem Rahmenwerk TIBER-EU, den Erfahrungen anderer Länder bei der nationalen Implementierung und unter Berücksichtigung des „Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector".[6,7] Die Veröffentlichung ist für das Jahr 2020 geplant.

2 Stand: 27.11.2019.

3 TIBER-NL GUIDE – How to conduct the TIBER-NL test, November 2017, https://www.dnb.nl/binaries/TIBER-NL Guide Second Test Round final_tcm46-365455.pdf, abgerufen am 3.12.2019.

4 TIBER-NL goes Europe, https://www.dnb.nl/en/news/nieuwsbrief-betalingsverkeer/Juni2018/index.jsp, abgerufen am 3.12.2019.

5 DNBulletin: DNB's TIBER programme: the next steps, https://www.dnb.nl/en/news/news-and-archive/DNBulletin2018/dnb379565.jsp, abgerufen am 3.12.2019.

6 Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector, https://eiopa.europa.eu/Publications/JC%202019%2025%20(Joint%20ESAs%20Advice%20on%20a%20coherent%20cyber%20resilience%20testing%20framework).pdf, abgerufen am 3.12.2019.

7 Vgl. BaFinJournal April 2019 Seite 26 ff.

3 Nationales Rahmenwerk TIBER-DE

TIBER-DE-Tests sollen Banken, Versicherungen, Finanzmarktinfrastrukturen und ihren wichtigsten Dienstleistern – auf freiwilliger Basis – offenstehen. Von den bedeutendsten Unternehmen des Finanzsektors wird jedoch erwartet, dass sie von diesem innovativen Instrument Gebrauch machen, um ihren Beitrag für die Cyber-Resilienz des gesamten Sektors zu leisten.

Bei der Implementierung des europäischen Rahmenwerks in Deutschland (siehe Abbildung 1, Seite 51) wird das Kompetenzteam der nationalen Umsetzung von TIBER-DE-Tests, das sogenannte TIBER Cyber Team (TCT, siehe Infokasten), bei der Deutschen Bundesbank im aufsichtsfernen Bereich Zahlungsverkehr und Abwicklungssysteme – und damit außerhalb der Bankenaufsicht – angesiedelt.[8] Da TIBER-DE grundsätzlich als freiwilliges Instrument konzipiert wurde, hat die Bundesbank eine klare organisatorische Trennung von TIBER-DE und der Bankenaufsicht im eigenen Hause vorgenommen. Dadurch wird sichergestellt, dass Informationen nur über die hierfür vorgesehenen Wege an die Aufsicht gelangen.

Die Steuerung von TIBER-DE erfolgt durch einen Lenkungsausschuss, dem BaFin und die Deutsche Bundesbank angehören. Dieser arbeitet derzeit intensiv an der konkreten Ausgestaltung des Rahmenwerks TIBER-DE. Zu seinen Aufgaben gehören weiterhin die Formulierung strategischer Ziele und die Weiterentwicklung von TIBER-DE. Eine Einbindung des Lenkungsausschusses in die einzelnen TIBER-DE-Tests erfolgt aufgrund seiner strategischen Ausrichtung nicht.

Ausgangsbasis für die nationale Implementierung von TIBER-EU ist das TIBER-EU Framework[9], das die Vorgehensweise der nationalen Adaption und Implementierung des Rahmenwerks sowie die einzelnen Phasen, Aktivitäten und zu erstellenden Dokumente eines TIBER-Tests beschreibt.

Definition

TIBER Cyber Team

Das TIBER Cyber Team (TCT) stellt das nationale Kompetenzzentrum einer TIBER-Implementierung dar. In Deutschland ist diese Einheit bei der Bundesbank angesiedelt. Dieses Cyber-Team begleitet die von Unternehmen beauftragten TIBER-Tests während des kompletten Verlaufs, unterstützt sie mit Fachwissen, sorgt für die Einhaltung der Rahmenbedingungen von TIBER-Tests und stellt die Kommunikationsschnittstelle nach außen dar. Dem TCT obliegt das Recht, einen Test als nicht TIBER-konform einzustufen, wenn dieser nicht im Einklang mit dessen Anforderungen durchgeführt wurde.

Der Team Test Manager (TTM) ist ein Mitglied des TCT, der ein spezifisches Unternehmen bei einem TIBER-Test betreut und die Schnittstelle zu diesem bildet. Der TTM betreut das Unternehmen während der gesamten Laufzeit eines Tests.

Der Prozess eines TIBER-Tests besteht aus einer optionalen sowie drei obligatorischen Phasen (siehe Abbildung 1), die auf Seite 51 dargestellt werden.

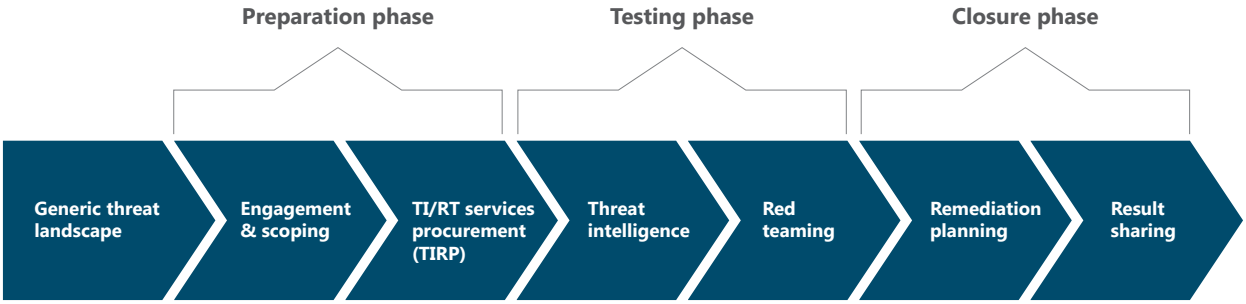
Generische Bedrohungslage
Mit der (optionalen) generischen Bedrohungslage (Generic Threat Landscape) wird ein Lagebild zu den Risiken und Bedrohungen für den gesamten (nationalen) Finanzsektor erstellt. Maßgebliche potenzielle Angreifer und ihre spezifischen Techniken, Taktiken und Vorgehensweisen werden dem Grundsatz nach analysiert. Die geeignete Vorgehensweise, eine generische Bedrohungslage für TIBER-DE zu erstellen, evaluieren die beteiligten Behörden im weiteren Verlauf der Implementierung.

Vorbereitungsphase
In der Vorbereitungsphase (Preparation Phase) beginnen die Planungen für den TIBER-Test, das Launch-Meeting mit Beteiligung des TIBER Cyber Teams und optional

8 Pressemitteilung „TIBER-DE macht das deutsche Finanzsystem sicherer", https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2019/09/2019-09-12-Tiber-de.html, abgerufen am 3.12.2019.

9 TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, May 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf, abgerufen am 3.12.2019.

Abbildung 1: Der TIBER-EU-Prozess



Quelle: Europäische Zentralbank, TIBER-EU Framework, Mai 2018, Seite 20, Abbildung 3.

auch der BaFin findet statt, der Testumfang wird bestimmt und die externen Test-Dienstleister werden vom Unternehmen beauftragt.

Die Deutsche Bundesbank benennt den TIBER Test Manager (TTM) aus dem TIBER Cyber Team als zuständigen Ansprechpartner für das Unternehmen und das Unternehmen stellt wiederum das White Team (WT)[10] auf.

Das White Team ist die für die Durchführung eines TIBER-DE-Tests verantwortliche Instanz im Unternehmen, wird von dessen Geschäftsleitung eingesetzt und bildet die Schnittstelle zum TIBER Test Manager. Innerhalb des Unternehmens darf lediglich das White Team über den geplanten Test informiert sein; insbesondere die mit der Abwehr von Cyberangriffen befassten Arbeitseinheiten (Blue Team) dürfen dabei nicht gewarnt werden, da ansonsten die Aussagekraft des Tests deutlich eingeschränkt würde. Das White Team legt in dieser Phase den Rahmen und die Zielsetzung des Tests fest, die von der Geschäftsleitung des Unternehmens freigegeben und dem TIBER Test Manager und der BaFin übermittelt werden. Im Fokus des Tests sollen die kritischen Systeme und Prozesse stehen.

In dieser Phase nimmt das White Team auch die Risikobewertung und die Etablierung der entsprechenden Risikomanagementkontrollen für den TIBER-DE-Test vor. Ein aktives und robustes Risikomanagement ist ein wesentliches Element eines TIBER-DE-Tests und liegt in der Verantwortung des Unternehmens. Dies ist besonders wichtig, da bei solch einem Test die produktiven, kritischen Systeme des Unternehmens geprüft werden und daher ein Risiko von Störungen oder Ausfällen dieser Systeme besteht.

Abschließend beauftragt das Unternehmen die Dienstleister – Threat Intelligence Team (TIT) und Red Team (RT), die beiden zentralen Akteure eines TIBER-Tests (vgl. Abbildung 2, Seite 53). Red Team und Threat Intelligence Team müssen im Sinne von TIBER-EU unabhängige und externe Dienstleister sein, welche die Anforderungen der im Rahmen von TIBER-EU veröffentlichten Services Procurement Guidelines erfüllen. TIBER-EU[11] sieht hierbei explizit den Einsatz von externen Red Teams vor, da diese unter Umständen alternative Vorgehensweisen, Werkzeuge oder Erkenntnisse bei der Testdurchführung einsetzen, die interne Tester womöglich übersähen oder missachteten. Interne Experten dürfen externe Tester in einem ausgewogenen Maß unterstützen.

10 TIBER-EU White Team Guidance – The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test", December 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf, abgerufen am 3.12.2019.

11 TIBER-EU FRAMEWORK – Services Procurement Guidelines", August 2018. https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf, abgerufen am 3.12.2019.

Da die externen Dienstleister während des Tests sowohl fundierte Kenntnisse über die Cybersicherheit der Unternehmen erhalten, als auch auf deren Produktivsystemen testen, ist bei ihrer Auswahl große Sorgfalt geboten, um mögliche Risiken zu vermeiden.

Testphase
Noch vor Beginn der eigentlichen Testphase (Testing Phase) erstellt das Threat Intelligence Team den sogenannten Targeted Threat Intelligence Report für das jeweilige Unternehmen. Dieser Bericht, der – soweit vorhanden – auf der generischen Bedrohungslage basiert, stellt wiederum die unternehmensspezifische Bedrohungslage dar. Er umfasst mögliche Angriffsszenarien und Schwachstellen sowie weitere nützliche Informationen über das Unternehmen. Der Bericht zur unternehmensspezifischen Bedrohungslage wird den relevanten Stellen im Unternehmen, dem TIBER Test Manager und dem Red Team zur Verfügung gestellt und mit ihnen diskutiert. In Anlehnung an das Vorgehen bei anderen nationalen Implementierungen werden für TIBER-DE noch weitere denkbare Maßnahmen zur Qualitätssicherung und Anreicherung des Berichts zur unternehmensspezifischen Bedrohungslage geprüft.

Das Red Team leitet aus diesem Bericht konkrete Angriffsszenarien ab und führt die Angriffe unter Berücksichtigung der festgelegten Zielsetzung auf kritische Systeme, organisatorische Strukturen und Prozesse des Unternehmens aus. Erzielt das Red Team keine Fortschritte bei seinen Angriffen, sieht das TIBER-EU-Rahmenwerk vor, dass das White Team das Red Team fachlich unterstützt. So soll eine Überprüfung möglichst aller Systeme, die für die Zielerreichung bedeutend sind, gewährleistet werden.

Das im Vorfeld des Tests vom Unternehmen speziell dafür eingerichtete Risikomanagement hat während des Tests darauf zu achten, dass die Maßnahmen und Überwachungsinstrumente zur Risikominimierung wirksam sind. Aus diesem Grund muss das Red Team das White Team eng in den Ablauf des Tests einbinden. Weiterhin ist der TIBER Test Manager regelmäßig – mindestens einmal wöchentlich – über den Testfortschritt zu informieren.

Abschlussphase
In der Abschlussphase (Closure Phase) des TIBER-DE-Tests werden die Resultate analysiert, Folgemaßnahmen vereinbart und alle Ergebnisse an die im TIBER-DE-Rahmenwerk festgelegten Stellen kommuniziert.

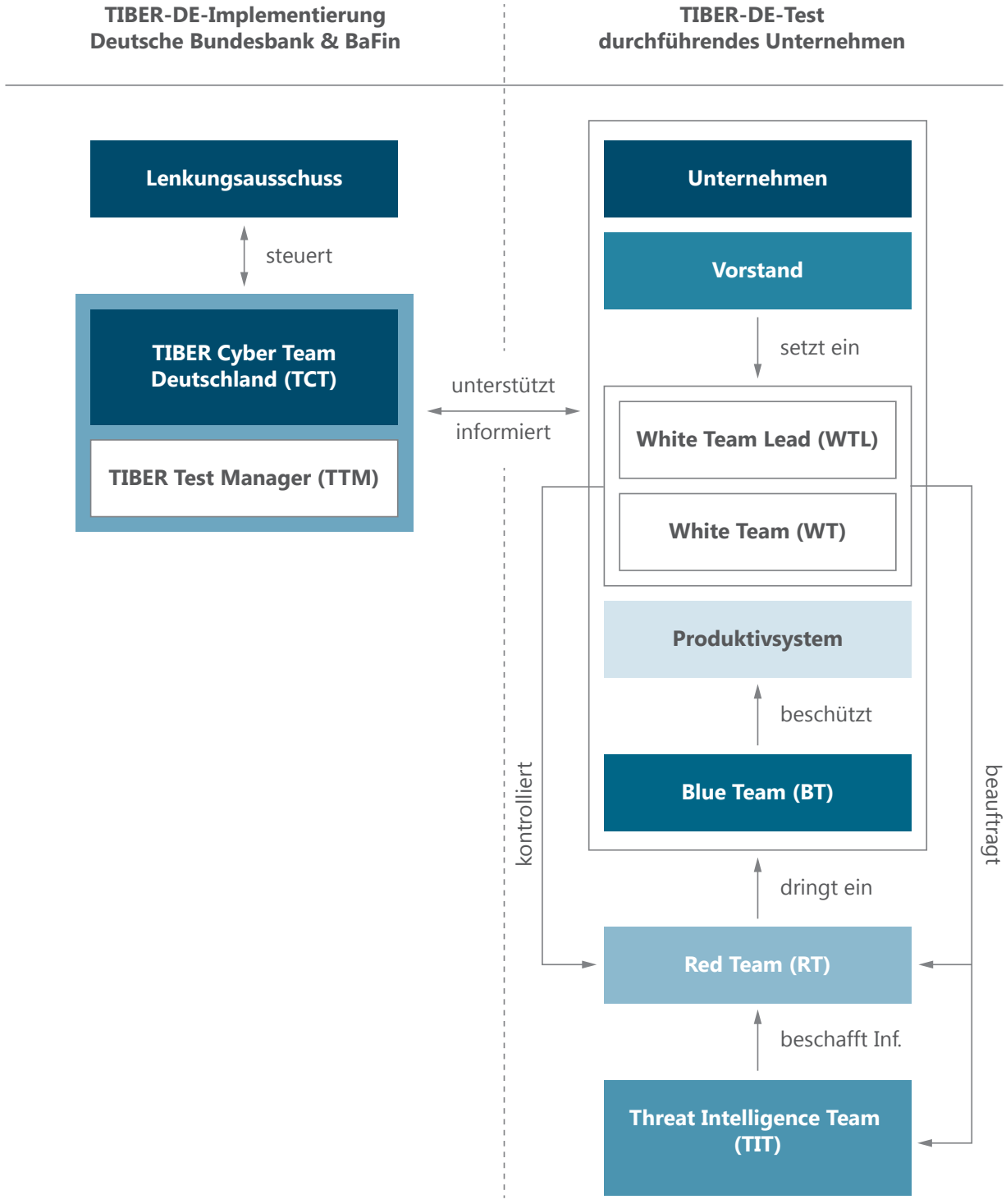
Zu Beginn dieser letzten Phase eines TIBER-DE-Tests findet ein 360-Grad-Feedbacktreffen aller Beteiligter unter Einbindung des TIBER Test Managers statt. In diesem Gespräch werden die Testergebnisse analysiert. Weiterhin erstellt das Red Team einen Test Summary Report, der die Vorgehensweise und Ergebnisse darstellt. Falls notwendig, soll der Bericht auch detaillierte Informationen enthalten, wie sich Abwehrmechanismen (zum Beispiel in Bezug auf physische oder technische Sicherheitsvorkehrungen, Unternehmensrichtlinien und -abläufe, Sensibilisierung und Ausbildung der Mitarbeiter) künftig verbessern lassen können. Dieser Report wird dem TIBER Test Manager zur Verfügung gestellt.

Im Rahmen der strategischen Ausrichtung von TIBER-DE wird zurzeit über die Etablierung des optionalen Purple Teamings in der Abschlussphase eines Tests im Rahmen der Erstellung des nationalen Rahmenwerks diskutiert. Hierbei treten Blue Team und Red Team in einen Dialog, um über Angriffe, weitere Angriffsmöglichkeiten und Abwehrschritte, die das Unternehmen für diese Fälle vorsieht, zu diskutieren. Dieser Austausch kann wesentlich dazu beitragen, Lehren (Lessons Learned) aus dem TIBER-DE-Test zu ziehen.

Abschließend erstellt das Unternehmen einen Maßnahmenplan (Remediation Plan), um die im Test identifizierten Schwachstellen zu beheben.

Die Ergebnisse der TIBER-DE-Tests sind dabei sowohl für die technischen Experten der Unternehmen als auch für die Managementebene von hoher Bedeutung: Auf der einen Seite werden Schwachstellen im Bereich der Cybersicherheit aufgedeckt und können adäquat behoben werden. Auf der anderen Seite werden die Auswirkungen von Cyberangriffen anschaulich dargestellt und die konkreten Auswirkungen (zum Bespiel Abfluss sensibler Informationen, Änderungen von Daten) illustriert.

Abbildung 2: Akteure und Rollen bei TIBER-DE-Implementierung und TIBER-DE-Tests



Quelle: Deutsche Bundesbank

4 Fazit

TIBER-DE-Tests unterstützen Unternehmen dabei, ihre Cyber-Resilienz realitätsnah zu prüfen und die Auswirkungen möglicher Cyberangriffe darzustellen. Nach der deutschen Implementierung des TIBER-EU Rahmenwerks haben die Unternehmen die Möglichkeit, bedrohungsgeleitete ethische Penetrationstests zu absolvieren. Aufgrund der Anforderungen des Rahmenwerks ist eine hohe Qualität der Tests sichergestellt und ihre Anerkennung in mehreren Ländern möglich. Durch eine enge Zusammenarbeit zwischen den beteiligten Behörden und den Unternehmen soll in einem kooperativen Ansatz die Cyber-Resilienz im gesamten Finanzsektor erhöht werden, um den mit der Digitalisierung einhergehenden Gefahren angemessen zu begegnen.

„Die Bedrohung ist da. Und sie wächst.“

Interview mit

Raimund Röseler
Exekutivdirektor Bankenaufsicht,
Bundesanstalt für Finanzdienstleistungsaufsicht
(BaFin)

Viele Daten, viel Geld – beides macht den Finanzsektor für Cyberkriminelle zu einer beliebten Zielscheibe. Die Corona-Pandemie könnte das Problem nach Ansicht von Raimund Röseler sogar noch verschärfen. Der Exekutivdirektor Bankenaufsicht weiß aber auch: Die meisten IT-Schäden werden nach wie vor versehentlich angerichtet – und zwar bei den IT-Dienstleistern, aber auch intern durch schadhafte Hardware oder die eigenen Angestellten. Die sind in der Corona-Krise sogar besonders anfällig für Fehler, denn Arbeitsbedingungen und Prozessabläufe sind anders als sonst.

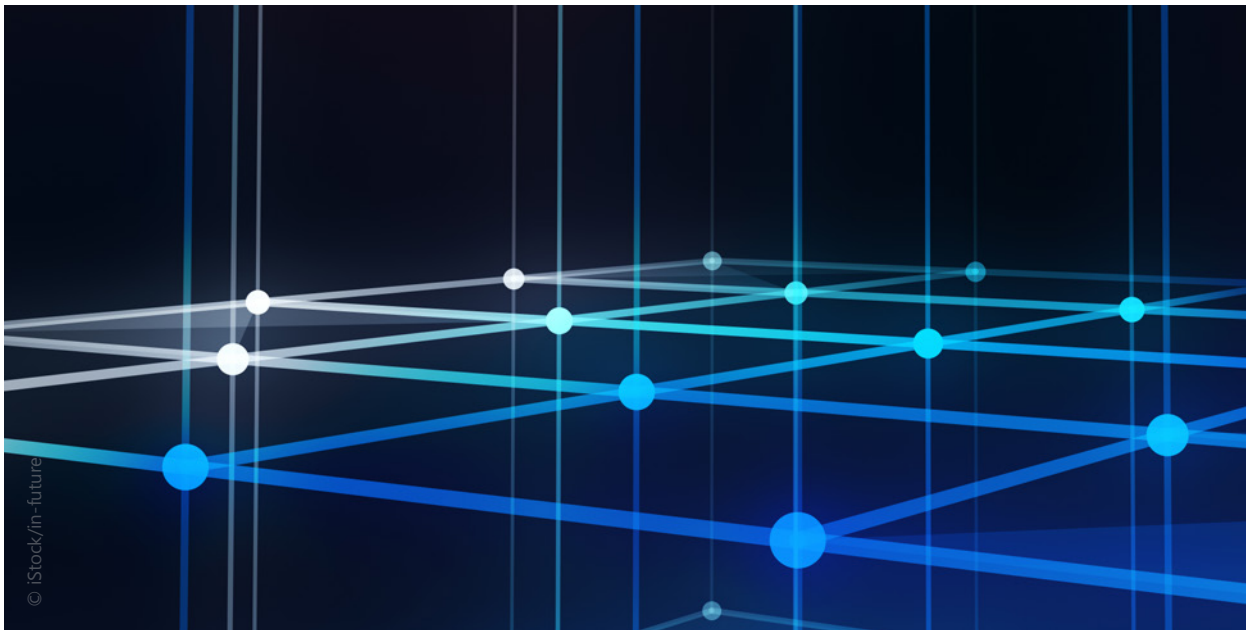
Röseler erläutert im Interview mit den BaFinPerspektiven, worauf es ankommt, wenn Banken und andere Zahlungsdienstleister Opfer von Cyberangriffen oder internen IT-Pannen werden, und an welchen Stellen die Regulierung noch nachgebessert werden sollte.

Herr Röseler, wie erfährt die BaFin überhaupt von Cyberangriffen oder IT-Pannen?
Zahlungsdienstleister wie etwa Banken müssen uns seit 2018 schwerwiegende Cybervorfälle melden – genauer gesagt: schwerwiegende Betriebs- oder Sicherheitsvorfälle (siehe Infokasten, Seite 56). Das sind Attacken von außen oder Sabotageakte von Beschäftigten, aber auch interne Pannen, bei denen kein Vorsatz im Spiel ist.

Eine Meldepflicht gibt es auch für Betreiber kritischer Infrastrukturen des gesamten Finanzsektors. Adressat ist da allerdings das Bundesamt für Sicherheit in der Informationstechnik (BSI).[1] Das BSI reicht uns aber die Meldungen weiter, wenn Unternehmen betroffen sind, die wir beaufsichtigen. Wir sind also auch im Bilde.

Was aber fehlt, sind die Versicherer und der Wertpapiermarkt.
So ist es. Wir haben in der Versicherungs- und der Wertpapieraufsicht keine flächendeckenden Meldepflichten. Da sind also noch weiße Flecken auf der Informationslandkarte.[2] Es gibt aber zum Glück erste Ansätze, sie zu beseitigen und die Meldepflichten zu harmonisieren. Bei der Gelegenheit will man eventuell auch bestehende Pflichten vereinfachen. Die EU-Kommission hat im Dezember 2019 eine erste Konsultation in Form eines Fragebogens[3] dazu durchgeführt.

1 Vgl. Seite 55 ff.
2 Vgl. Seite 69 ff.
3 EU-Kommission, Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf, abgerufen am 7.5.2020.



Auf einen Blick

Cybervorfall

Ein Cybervorfall ist ein böswillig oder versehentlich herbei geführter Vorfall, der

- die Cybersicherheit eines Informationssystems oder die Sicherheit der verarbeiteten Informationen gefährdet oder
- Sicherheitsrichtlinien, Sicherheitsprozesse oder Nutzungsbedingungen verletzt.[4]

Ein böswillig herbeigeführter Cybervorfall kann ein externer Angriff sein, aber auch Sabotage innerhalb des Unternehmens. Davon zu unterscheiden sind interne Pannen, also Störungen, die Beschäftigte versehentlich herbeiführen. Auch solche internen Pannen werden unter dem Begriff „Cybervorfall" subsummiert.

Im Zahlungsdiensteaufsichtsgesetz (ZAG) ist nicht von Cybervorfällen die Rede, sondern von schwerwiegenden Betriebs- oder Sicherheitsvorfällen. Gemeint ist im Grunde das Gleiche, der Begriff „Cybervorfall" bezieht sich aber nicht nur auf Zahlungsdienstleister, sondern auf den gesamten Finanzsektor.

Meldepflicht

Das ZAG verlangt in § 54 Satz 1:

„Ein Zahlungsdienstleister hat die Bundesanstalt unverzüglich über einen schwerwiegenden Betriebs- oder Sicherheitsvorfall zu unterrichten. Die Bundesanstalt unterrichtet die Europäische Bankenaufsichtsbehörde und die Europäische Zentralbank unverzüglich nach Eingang einer Meldung über die maßgeblichen Einzelheiten des Vorfalls. Sie hat die Relevanz des Vorfalls für andere in ihrer sachlichen Zuständigkeit betroffene inländische Behörden unverzüglich zu prüfen und diese entsprechend zu unterrichten."

Lassen Sie uns einen Blick auf die Banken und anderen Zahlungsdienstleister werfen. Die müssen schwerwiegende Vorfälle ja seit 2018 melden. Können Sie Zahlen nennen – auch was die Schäden angeht?
Ja und nein. 680 schwerwiegende Fälle sind uns bislang gemeldet worden.[5] Der Schaden lässt sich nur schwer ermitteln. Da wären zum Beispiel der finanzielle Schaden des Instituts, sein Reputationsschaden, der Schaden des Kunden und – last but not least – der potentielle Schaden für die Finanzstabilität. Da gibt es keinen Automatismus, nach dem Motto ‚der Vorfall ist schwer, also ist der Schaden sehr groß'. Hier spielen andere Kriterien eine

4 Vgl. Financial Stability Board (FSB), Cyber lexicon, Seite 9, https://www.fsb.org/wp-content/uploads/P121118-1.pdf, abgerufen am 21.4.2020.

5 Stand 20. April 2020.

Rolle: die Größe des Instituts zum Beispiel, aber auch, wie lange ein Vorfall dauert oder wie relevant die betroffenen Systeme und Dienstleistungen sind.

Waren die schwerwiegenden Vorfälle Angriffe von außen?
Nur ein kleiner Teil davon. 14 der 680 gemeldeten Vorfälle, um genau zu sein. Die allermeisten Fälle hatten interne Ursachen: menschliches Versagen zum Beispiel, Fehler in den Prozessen oder den IT-Systemen.

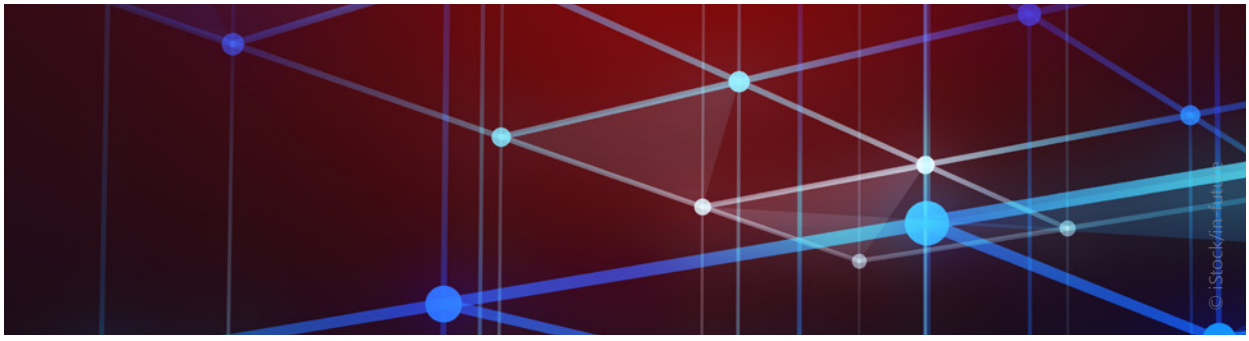
Werden seit Ausbruch der Corona-Pandemie mehr schwerwiegende Vorfälle gemeldet?
Bei den schwerwiegenden Fällen, die uns gemeldet werden, sehen wir im Moment noch keinen signifikanten Anstieg. Es kann aber gut sein, dass wir den irgendwann sehen werden. Sehr viele Menschen arbeiten von zu Hause aus, Arbeitsabläufe werden zunehmend digitalisiert, die IT-Infrastrukturen sind stark ausgelastet. Außerdem beflügelt die Corona-Krise offenbar flächendeckend, auch im Finanzsektor, die Cyberaktivität. Im April wurde zum Beispiel ein IT-Dienstleister in den USA Opfer eines erpresserischen Cyberangriffs, bei dem Daten verschlüsselt wurden. Davon waren zahlreiche US-amerikanische Banken betroffen.

Und wenn es zu einem Cyberangriff direkt auf einen Zahlungsdienstleister gekommen ist: Konnten die Unternehmen bisher damit umgehen?
Ja, die deutschen Finanzdienstleister, die Opfer von Cyberangriffen geworden sind, haben sich gut geschlagen. Was natürlich eine gute Nachricht ist. Was uns allerdings wichtig ist: Die Institute müssen ihre Krisenkommunikation immer wieder auf den Prüfstand stellen. Vor allem in den sozialen Medien verbreiten sich nämlich Nachrichten über Cybervorfälle wie ein Lauffeuer. Das sind dann oft mehr oder weniger haltlose Gerüchte. Die können dem betroffenen Institut sehr schaden.

Ansonsten haben die Zahlungsdienstleister im Krisenmanagement keinerlei Schwächen?
Soweit würde ich nicht gehen, aber in der Tat liegen die Schwächen der Institute eher in anderen Bereichen. Bei unserer IT- Prüfungskampagne 2019 vor Ort bei den kleineren und mittleren Banken[6] haben wir die größten Defizite im Informationsrisiko- und im Berechtigungsmanagement festgestellt. Auch im Informationssicherheits- und Auslagerungsmanagement gab es signifikante Defizite.

Zurück zum Krisenmanagement: Hat die BaFin dazu beigetragen, dass es bei den Unternehmen relativ gut funktioniert?
Ja, das sehe ich so. Wir verlangen von den Banken zum Beispiel, dass sie Notfallpläne für den Ernstfall parat haben. Die müssen sie immer wieder testen. Ein gutes Krisenmanagement ist das A und O. Noch hat es wenig Cyberangriffe gegeben, und die Banken haben sie gut überstanden. Aber die Bedrohung ist da. Und sie wächst. In unseren BAIT, den Bankaufsichtlichen Anforderungen an die IT, buchstabieren wir aus, wie ein Krisenmanagement beschaffen sein muss, um zu funktionieren. Vergleichbar hohe Anforderungen stellen wir auch in unseren VAIT und KAIT (siehe Infokasten, Seite 58).

6 So genannte weniger bedeutende Institute (Less Significant Institutions – LSIs).



Auf einen Blick

In drei Stufen zu mehr IT-Sicherheit

Für ihre IT-Aufsichtspraxis hat die BaFin ein Dreistufenprogramm entwickelt.

Stufe eins bildet ein Set von drei Rundschreiben, in denen für die Unternehmen der verschiedenen Aufsichtsbereiche vergleichbare Anforderungen an deren IT formuliert werden: die Bankaufsichtlichen Anforderungen an die IT (BAIT)[7], die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT)[8] und die Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT)[9].

In BAIT, VAIT und KAIT buchstabiert die BaFin aus, was sie von den Unternehmen in puncto IT-Governance und Informationssicherheit verlangt. Die BAIT konkretisieren § 25a Kreditwesengesetz, die VAIT § 23 Versicherungsaufsichtsgesetz und die KAIT § 28 Kapitalanlagegesetzbuch. In allen drei Rundschreiben hat die BaFin klargestellt, dass IT-Sicherheit Chefsache ist. Ziel dieser Rundschreiben ist deshalb auch, in den Vorstandsetagen das Bewusstsein für IT-Risiken zu schärfen, auch mit Blick auf Risiken, die bei der Ausgliederung oder dem Erwerb von IT-Dienstleistungen entstehen können.

Um Unsicherheiten bei Auslagerungen und Ausgliederungen an Cloud-Anbieter zu minimieren, hat die BaFin zusätzlich eine Orientierungshilfe[10] zu Auslagerungen an Cloud-Anbieter veröffentlicht.

Stufe zwei hat zum Ziel, die Einhaltung dieser Rundschreiben vor Ort zu prüfen. Zugleich zielt Stufe zwei darauf, die Widerstandsfähigkeit (Resilience) der Banken gegen Cyberangriffe und ihre Fähigkeit, den Geschäftsbetrieb aufrechtzuerhalten (Continuity), weiter zu stärken. Dazu nimmt die BaFin die Effektivität der bestehenden Sicherheitsvorkehrungen verstärkt in den Fokus. Zu Stufe zwei gehören auch Red-Teaming-Tests[11], eine Art von Cyber-Stresstests für den deutschen Finanzsektor.

Auf **Stufe drei** geht es um die Verbesserung des Krisenmanagements: Sowohl die Institute als auch die BaFin müssen jederzeit auf einen Cyberangriff oder einen IT-Betriebsvorfall vorbereitet sein. Die BaFin hat deshalb, die BAIT um ein Modul zum Notfallmanagement inklusive Notfalltests erweitert. Zusätzlich finden Cyberübungen statt, bei denen alle relevanten Akteure das Zusammenspiel im Krisenfall proben – und das national wie international. Der geplante „Krisenplan Cyber" ist ebenfalls auf Stufe drei angesiedelt (siehe Infokasten, Seite 59).

Was kann die BaFin tun, wenn es zum Beispiel bei einer Bank zu einem Cybervorfall kommt?
Wir können auf mehreren Wegen aktiv werden. Wir sorgen zum Beispiel dafür, dass uns das Unternehmen umfassend und fortlaufend über den Stand der Dinge informiert. Wir können Pressemitteilungen veröffentlichen, um für einen sachlichen Umgang mit dem Vorfall zu sorgen – auch in den sozialen Medien. Und wir unterstützen den Austausch von Betroffenen untereinander, um so die Behebung eines Vorfalls zu beschleunigen.

Was auch sehr wichtig ist: Wir schließen uns eng mit den anderen beteiligten Institutionen zusammen – mit dem BSI zum Beispiel, der Europäischen Zentralbank, der Deutschen Bundesbank und dem Bundesfinanzministerium. Denn es geht auch darum, Schäden für die Finanzstabilität zu verhindern. Bei schwerwiegenden

7 www.bafin.de/dok/10171976.
8 www.bafin.de/dok/11101474.
9 www.bafin.de/dok/13068070.
10 www.bafin.de/dok/11681122.
11 Vgl. auch Seite 50 ff.

Vorfällen informieren wir auch das Nationale Cyber-Abwehrzentrum. Wir können auch die Strafverfolgungsbehörden mit ins Boot holen. Oder unsere Kollegen in den G-7-Staaten – das machen wir allerdings nur, sollte ein Cybervorfall internationale Dimensionen entwickeln. Dieses Netzwerk aus verschiedenen Institutionen ist für uns sehr wichtig.

Hilft die BaFin den Unternehmen beim Zusammenkehren der Scherben?
Nein, wir sind nicht die technischen Ausputzer. Das ist nicht unsere Aufgabe, und dazu fehlt uns auch die Expertise. Das machen die Unternehmen selbst oder Anbieter, die sich auf sowas spezialisiert haben. Davon abgesehen hat jeder Finanzdienstleister seine technischen Eigenheiten. Die wissen dann meist selbst am besten, wie sie das Problem angehen müssen.

Unser Part ist ein anderer: Wir wollen dazu beitragen, die Auswirkungen eines Cybervorfalls abzumildern. Unter anderem mit den Mitteln, die ich gerade angesprochen habe. Die Betroffenen vernetzen, den Markt mit sachlichen Informationen versorgen und so weiter.

Gerade war von einem IT-Dienstleister in den USA die Rede. Kann die BaFin aktiv werden, wenn das Problem nicht bei einer Bank oder einem Versicherer liegt, sondern bei deren IT-Dienstleister?
Da sprechen Sie ein wichtiges Thema an. Auch an der Stelle haben wir noch keine Einheitlichkeit. In der Versicherungsaufsicht haben wir direkte Befugnisse gegenüber Drittdienstleistern. In der Bankenaufsicht prüfen wir zwar auch Drittdienstleister, sind aber nicht ganz so gut aufgestellt. Wir überlegen derzeit, ob und wie man die Rahmenbedingungen in Deutschland ändern und vereinheitlichen sollte. Generell müssen wir uns fragen, wie wir angemessen mit der Relevanz beziehungsweise Systemrelevanz von großen IT-Drittdienstleistern umgehen, auf die viele Banken und Versicherer auslagern. Diese Frage sollten wir uns aber idealerweise nicht nur in Deutschland stellen, sondern auch in Brüssel.

Nehmen wir an, dass mehrere Banken betroffen sind – oder sogar Banken und Versicherer oder andere Finanzdienstleister. Wäre die BaFin gerüstet?
Das ist bislang nicht vorgekommen, wäre aber wohl ein Beispiel für eine Cyberkrise und damit ein Fall für unseren „Krisenplan Cyber". Den wollen wir hausweit etablieren und sind gerade in der Feinabstimmung.

In einer Cyberkrise (siehe Infokasten, Seite 59) kämpfen wir auch gegen die Zeit. Wir müssen innerhalb kurzer Zeit reagieren und die richtigen Entscheidungen treffen können. Da müssen wir aus dem Stand mit allen Beteiligten kommunizieren und uns untereinander abstimmen können. Blitzschnell und reibungslos. Sowas kann man nicht dem Zufall überlassen, da muss jede Bewegung sitzen. Aus dem Grund haben wir den „Krisenplan Cyber" entwickelt. Ich denke, damit sind wir gut gerüstet. Wie gesagt, wir hatten noch keine Cyberkrise und mussten den Krisenplan auch noch nicht aus der Schublade ziehen. Aber wir haben ihn mehrmals mit Erfolg durchgespielt – auch unter kritischen externen Blicken.

Defintion

Was ist eine Cyberkrise?

Der „Krisenplan Cyber" definiert eine Cyberkrise als einen Cybervorfall (siehe Infokasten, Seite 56), der Funktionen eines oder mehrerer beaufsichtigter Unternehmen beeinträchtigt,

- deren fehlende Ausübung die Realwirtschaft oder das Finanzsystem gefährden oder
- deren plötzlicher Ausfall wahrscheinlich wesentliche Auswirkungen auf Dritte hat oder zur Ansteckung führt oder das allgemeine Vertrauen der Marktteilnehmenden untergraben könnte.

Drehen wir das Rad noch etwas weiter: Wie reagiert die BaFin, wenn aus einer Cyberkrise eine, sagen wir, klassische Krise wird? Eine Liquiditätskrise zum Beispiel.
Das wäre nicht auszuschließen, und wir bilden solche Entwicklungen in unserem „Krisenplan Cyber" auch ab. Für die so genannten klassischen Krisen haben wir in der BaFin ohnehin schon Krisenpläne. Seit langem. Mit denen verknüpfen wir unseren Cyber-Krisenplan. Unser

Ziel ist, dass wir auch bei solchen Entwicklungen sofort entscheidungs- und handlungsfähig sind. Es muss klar sein, wer wen worüber informiert, wer welche Entscheidungen trifft und so weiter. Auch da sind wir gut aufgestellt. Aber am liebsten wäre mir, wenn es soweit gar nicht käme.

Man kann es gar nicht oft genug sagen: Wir brauchen ein gut funktionierendes Krisenmanagement – bei den Unternehmen und bei uns. Aber wir brauchen auch eine gute Abwehr. An beides – Krisenmanagement und Abwehr – stellen wir in unseren Rundschreiben BAIT, VAIT und KAIT daher auch hohe Anforderungen (siehe Infokasten, Seite 58).

Von der Cyberkrise über die klassische Krise zur Systemkrise: Der Europäische Ausschuss für Systemrisiken hat im Februar 2020 Cyberrisiken als mögliches Risiko für das gesamte Finanzsystem eingestuft.[12] Der Ausschuss für Finanzstabilität hat schon 2019 Cyberrisiken als systemische Risiken für Deutschland identifiziert. Wie könnte ein systemischer Vorfall aussehen?
Von einem systemischen Vorfall würde ich reden, wenn kritische Dienstleistungen des Finanzsektors wegen einer IT-Störung nicht mehr zur Verfügung stehen. Der Grund könnte eine Cyberattacke sein, aber auch eine interne Panne. Stellen Sie sich folgendes vor: Die Karten eines großen Instituts funktionieren nicht mehr, weil irgendwas versehentlich falsch konfiguriert worden ist. Die Kunden dieses Instituts wären von jetzt auf gleich nicht mehr zahlungsfähig. Da kommt Freude auf, wenn Sie gerade vollgetankt haben oder mit einem Rieseneinkauf an der Supermarktkasse stehen. Oder wenn Sie als Dienstleister dringend eine Warenlieferung brauchen.

Wenn so etwas passiert, ist für die Finanzstabilität entscheidend, wie lange die Störung anhält. Dauert der Vorfall lange oder befinden wir uns ohnehin schon in einer Krise – man denke nur an die Corona-Pandemie – dann können die Auswirkungen für die Kunden gravierend sein. Da müssten wir dann zur Not einschreiten.

Was die Sache noch verschlimmern könnte: Die Kunden anderer Banken könnten nervös werden und Geld abziehen, weil sie Angst haben, später keines mehr abheben zu können. Dann ließe der gefürchtete Bank-run nicht mehr lange auf sich warten. Und dann könnten auch Institute in Liquiditätsengpässe geraten, die eigentlich nichts mit dem IT-Vorfall zu tun hatten.

Gab es solche systemischen Vorfälle schon?
Wir hatten schon Vorfälle, bei denen kritische Funktionen einer großen Bank oder einem ganzen Verbund an Banken lahmgelegt waren. Sie waren aber zeitlich sehr eng begrenzt und den Betroffenen ist es gelungen, rechtzeitig gegenzusteuern und die Auswirkungen früh genug einzudämmen. Außerdem haben die Informationskanäle, die ich gerade beschrieben habe, sehr gut funktioniert.

Herr Röseler, wir danken Ihnen für das Interview!

Das Interview führte Ursula Mayer-Wanders, Gruppe Kommunikation. Mitgewirkt haben Theresa Nabel und Dr. Sebastian Silberg, beide Gruppe IT-Aufsicht.

12 Pressemeldung des ESRB, ESRB publishes report on systemic cyberattacks, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html, abgerufen am 30.4.2020.

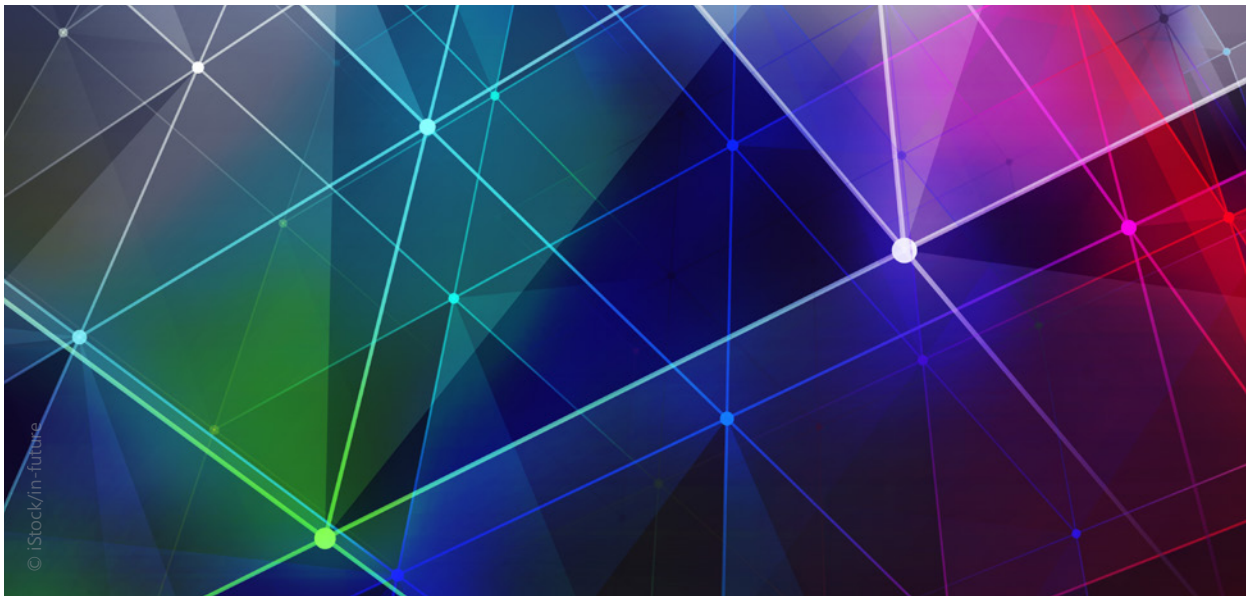
Aufsicht über Kritische Infrastrukturen im Finanzwesen – ein Überblick über den Status quo

Autor

Dr. Wolfgang Finkler
Referat WG 14 – KRITIS-Sektoren Finanz- und Versicherungswesen, IT und TK sowie Digitale Dienste, Bundesamt für Sicherheit in der Informationstechnik (BSI)

1 Einleitung

Mit dem IT-Sicherheitsgesetz aus dem Jahr 2015 hat der Gesetzgeber die Grundlage dafür geschaffen, Betreiber Kritischer Infrastrukturen in Bezug auf die IT-Sicherheit ihrer Anlagen zu kontrollieren. Zu den Kritischen Infrastrukturen im Sinne des Gesetzes zählen auch Anlagen aus dem Finanz- und Versicherungswesen. Sie unterliegen zum Teil schon der Regulierung durch das Kreditwesengesetz (KWG), das Zahlungsdiensteaufsichtsgesetz (ZAG) oder das Versicherungsaufsichtsgesetz (VAG).



2 Überblick über die regulierten Aufsichtsobjekte Kritischer Infrastrukturen im Finanzwesen

Mit Inkrafttreten der ersten Verordnung zur Änderung der vom Bundesministerium des Innern erlassenen BSI-Kritisverordnung[1] im Juni 2017 können Kritische Infrastrukturen auch für den Sektor Finanz- und Versicherungswesen bestimmt werden. Es wurden fünf kritische Dienstleistungen sowie Anlagenkategorien, Bemessungskriterien und Schwellenwerte festgelegt, anhand deren Unternehmen oder Institutionen selbst feststellen können, ob sie Betreiber einer Kritischen Infrastruktur sind. Beispielsweise gibt es für die kritische Dienstleistung des „konventionellen Zahlungsverkehrs" die Anlagenkategorie eines „Kontoführungssystems" mit dem Bemessungskriterium „Anzahl dienstleistungsbezogener Transaktionen pro Jahr" und dem Schwellenwert 100 Millionen. Das heißt, dass alle Kontoführungssysteme, über die mehr als 100 Millionen Transaktionen pro Jahr abgewickelt werden, als Kritische Infrastruktur im Sinne des Gesetzes gelten und entsprechend abgesichert werden müssen.

Nachfolgend wird in diesem Beitrag ausschließlich auf die kritischen Dienstleistungen der Bargeldversorgung, des kartengestützten Zahlungsverkehrs und des konventionellen Zahlungsverkehrs Bezug genommen. Hier ist für den Begriff des „Betreibers" einer Kritischen Infrastruktur relevant, welches Unternehmen „unter Berücksichtigung der tatsächlichen Umstände bestimmenden Einfluss" auf die Anlage hat, die zur Erbringung der kritischen Dienstleistung genutzt wird, das heißt, wer die tatsächliche Sachherrschaft ausübt.[2]

Nachdem sie selbst festgestellt haben, dass sie Betreiber einer Kritischen Infrastruktur sind, und sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert haben, steht nun insgesamt eine Gruppe von circa 90 Unternehmen im Finanzwesen unter Aufsicht des BSI. In dieser Gruppe sind Institute bzw. Zahlungsdienstleister enthalten, die gemäß § 1 Absatz 1 KWG bzw. gemäß § 1 Absatz 1 ZAG der Aufsicht der BaFin unterfallen oder gemäß SSM-Verordnung[3] der Aufsicht durch die Europäische Zentralbank (EZB) unterliegen. Des Weiteren gibt es IT-Dienstleister, die Zahlungsverkehrsservices für Institute gemäß § 25b KWG bzw. § 20 Absatz 1 ZAG erbringen und daher der mittelbaren Aufsicht durch die BaFin unterfallen. Schließlich gehören auch Unternehmen zu dieser Gruppe, die Zahlungsverkehrsservices im Rahmen der Zahlungsverkehrs-Wertschöpfungskette erbringen und nicht der mittelbaren Aufsicht der BaFin unterfallen. Diese werden ausschließlich durch das BSI beaufsichtigt.

1 Bundesgesetzblatt Teil I Nr. 40, 29.6.2017, Seite 1903 ff.
2 Bundesgesetzblatt Teil I Nr. 40, 29.6.2017, Seite 1904, Paragraph 7, Absatz 8.
3 Verordnung (EU) Nr. 1024/2013, Amtsblatt der Europäischen Union L 287/63, 29.10.2013. Das Akronym SSM steht für Single Supervisory Mechanism (Einheitlicher Aufsichtsmechanismus), zu dem auch die BaFin zählt. Die bedeutenden Institute (Significant Institutions – SIs) stehen im Rahmen des SSM unter direkter Aufsicht der EZB. Die so genannten weniger bedeutenden Institute (Less Significant Institution – LSIs) stehen unter nationaler Aufsicht.

3 Begleitung der Betreiber Kritischer Infrastrukturen

Wie begleiten die Aufsichtsbehörden die Betreiber Kritischer Infrastrukturen bei der Vorbereitung auf die gesetzlichen Anforderungen des § 8a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)? Es soll an dieser Stelle zunächst auf Angebote und Wege eingegangen werden, welche die Betreiber Kritischer Infrastrukturen in der Finanzbranche zur Erfüllung ihrer präventiven Pflichten gemäß § 8a Absatz 1 BSIG gewählt haben.

Gemäß § 8a Absatz 1 BSIG sind Betreiber Kritischer Infrastrukturen verpflichtet, „spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht."

B3S – branchenspezifische Sicherheitsstandards

Wie es allgemein für alle Sektoren und Branchen möglich ist, können Betreiber Kritischer Infrastrukturen sowie ihre Verbände branchenspezifische Sicherheitsstandards (B3S) für die zielgerichtete Formulierung der typischen Anforderungen und Maßnahmen der Prävention nach dem Stand der Technik ausarbeiten und dem BSI einreichen, damit dieses die Eignung der B3S feststellen kann. Dies trägt dem Umstand Rechnung, dass in den KRITIS-Sektoren eine gewisse Heterogenität der Branchen und deren spezifisch eingesetzter Technik bestehen kann. Die Eignung eines eingereichten B3S wird nach erfolgreicher Prüfung im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes, im Finanzsektor meist der BaFin, bzw. für Sozialversicherungsträger mit dem Bundesamt für Soziale Sicherung (BAS) festgestellt.

Typischerweise wird ein B3S in einem Branchenarbeitskreis der Öffentlich-Privaten Partnerschaft des UP KRITIS[4] vorbereitet. Das BSI hat zur Vorbereitung der Erstellung von B3S eine Orientierungshilfe zu erwünschten Inhalten und Anforderungen an B3S veröffentlicht[5]. Als Anhaltspunkte sowohl für Anforderungen als auch für konkretere Handlungsanweisungen zum Stand der Technik können eine Reihe relevanter Standards herangezogen werden, wie die Standards zur Informationssicherheit der ISO/IEC 27000-Familie, der IT-Grundschutz des BSI, PCI DSS, der BSI-Standard 100-4 und ISO 22301 zum Notfallmanagement – um nur einige zu nennen. Diese haben zum Ziel, dass die Betreiber Aspekte zu Absicherung oder Sicherstellung der Kontinuität des Betriebes beachten.

Für eine Teilmenge der technisch geprägten Anlagen Kritischer Infrastruktur im kartengestützten Zahlungsverkehr – unter anderem bei den Netzbetreibern der Deutschen Kreditwirtschaft (DK) für die in der BSI-Kritisverordnung formulierten Bereiche „Anbindung an Autorisierungssysteme aus Sicht des Terminalbetreibers und beim Einbringen von Transaktionen in den Zahlungsverkehr" – wurde dieser Weg beschritten. Das BSI hat die Eignung eines B3S festgestellt, der in erheblichem Umfang auf Elemente von PCI DSS[6] Bezug nimmt, indem

4 Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen.

5 BSI, Kritische Infrastrukturen – Orientierungshilfe gemäß § 8a (2), https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/Orientierungshilfe/Orientierungshilfe_node.html, abgerufen am 16.3.2020.

6 Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2.1, May 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf, abgerufen am 16.3.2020.

er diese als maßgeblich für den Stand der Technik darstellt, und um weitere Anforderungen ergänzt hat. Das bedeutet, dass das große Inventar an Anforderungen aus dem PCI DSS, das ein Betreiber Kritischer Infrastrukturen gegebenenfalls bereits bei einer Zertifizierung nach PCI DSS als erfüllt nachweisen kann, nun auch in der Nachweiserbringung gegenüber dem BSI auf Basis dieses branchenspezifischen Sicherheitsstandards berücksichtigt werden kann. Zudem müssen die Betreiber in ihrem Zulassungsverfahren als Netzbetreiber im electronic cash-System der Deutschen Kreditwirtschaft bereits Sicherheitsanforderungen erfüllen.

Zusätzliche Belastung bestmöglich reduzieren

Als Ausgangslage bei den kritischen Dienstleistungen des Zahlungsverkehrs im Finanzwesen ist festzustellen, dass einige Institute, die nun Betreiber Kritischer Infrastruktur mit den einhergehenden gesetzlichen Anforderungen geworden sind, bereits der institutionalisierten Aufsicht des Bundes über Kreditinstitute durch die BaFin und die Deutsche Bundesbank bzw. einer europäischen Bankenaufsicht im Rahmen des SSM unterliegen. Hier gelten bereits die im BaFin-Rundschreiben 10/2017 formulierten Bankaufsichtlichen Anforderungen an die IT (BAIT)[7], in denen für den Bankensektor die einschlägigen Normen in Bezug auf die Anforderungen an eine ordnungsgemäße IT-Geschäftsorganisation interpretiert werden. Die Präsidenten von BSI und BaFin haben die Branche in einem gemeinsamen Schreiben informiert[8], dass eine zusätzliche materielle Belastung von Instituten, die nun auch KRITIS-Betreiber sind, im Rahmen des rechtlich Vertretbaren möglichst gering gehalten werden soll. Die BaFin veröffentlichte danach ein in Abstimmung mit dem BSI entwickeltes KRITIS-Modul als Ergänzung der BAIT[9]. Darin werden zusätzliche Anforderungen an Institute, die KRITIS-Betreiber sind, formuliert. Ferner wird in Nr. 61 der BAIT in der Fassung vom 14. September 2018 die Möglichkeit aufgezeigt, im Rahmen der Jahresabschlussprüfung die gegenüber dem BSI erforderlichen Nachweise durch Erweiterung des Prüfungsauftrags vom Prüfer zu erlangen.

Schon weit vor der Ergänzung der BAIT hat das BSI für Betreiber Kritischer Infrastrukturen, die bereits ein bestehendes ISO-27001-Zertifikat vorweisen können, auf seiner Internetseite[10] formuliert, welche Rahmenbedingungen es für die Verwendung solcher Zertifikate beim Nachweis der Erfüllung der Anforderungen nach § 8a BSIG als notwendig erachtet. Damit hat das BSI eine Grundlage für eine möglichst einfache Umsetzung der Vorgaben der KRITIS-Regulierung geschaffen. Die vom BSI beschriebenen Rahmenbedingungen umfassen auch die Fragen des Geltungsbereichs der Zertifizierungen und die Frage der Berücksichtigung der KRITIS-Schutzziele[11], die auch in Nr. 57 der BAIT in der Fassung vom 14. September 2018 beschrieben sind. Zentrales Anliegen der KRITIS-Schutzziele ist, dass bei der Informationssicherheitsrisikobehandlung die Versorgungssicherheit der Bevölkerung sichergestellt wird. Zudem wird der geeignete Umgang mit Risiken beschrieben. So sollen die Institute angeben, dass sie Maßnahmen umgesetzt haben. Über eine geplante Umsetzung zu berichten, reicht nicht aus.

7 Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT (BAIT).

8 BaFin, Bankaufsichtliche Anforderungen an die IT Kritischer Infrastrukturen, www.bafin.de/dok/11327090, abgerufen am 16.3.2020.

9 BaFin, Kritische Infrastrukturen: BaFin ergänzt BAIT um Kritis-Modul, www.bafin.de/dok/11486774, abgerufen am 16.3.2020.

10 BSI, FAQ - Nutzung eines bestehenden ISO 27001 Zertifikates als Bestandteil eines Nachweises gemäß § 8a (3) BSIG, https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_ISO27001/faq_bsi_8a_ISO27001_node.html, abgerufen am 16.3.2020.

11 a.a.O. (Fn. 5).

4 Bisherige Erkenntnisse aus den Nachweisen der Betreiber Kritischer Infrastrukturen

Die gemäß § 8a Absatz 3 BSIG im Juni 2019 fälligen und beim BSI eingereichten Nachweise haben im Hinblick auf die im vorigen Abschnitt aufgezeigten alternativen Wege – Nutzung eines branchenspezifischen Sicherheitsstandards (B3S), des BAIT-Kritis-Moduls oder von Zertifikaten in einer Zusatzprüfung – deutlich gemacht, dass die Betreiber erwartungsgemäß bei der Erfüllung der Anforderungen des § 8a Absatz 1 BSIG sehr unterschiedlich vorgegangen sind.

Von kürzeren Zusatzprüfungen unter Einbeziehung existierender Zertifizierungen von Informationssicherheitsmanagementsystemen bis hin zu langen eigenständigen Prüfungen unterschieden sich die dem BSI mitgeteilten Prüfungsaufwände erheblich. Zudem sind einige Betreiber lediglich für eine kleine Zahl an Anlagen Kritischer Infrastruktur verantwortlich, während andere Unternehmen mehr als ein Dutzend Anlagen betreiben. Auch das führt zu unterschiedlichen Prüfungsaufwänden. In den Prüfungen war jeweils die Betrachtung des gesamten Geltungsbereichs der Kritischen Infrastruktur gefordert.

Relativ häufig hatten die Prüfer der KRITIS-Betreiber für die Prüfung selbst eine individuelle Prüfgrundlage entwickelt, die sie typischerweise aus den Themengebieten ableiteten, die in der Orientierungshilfe für die Erstellung eines B3S enthalten sind.

Bei vielen der durch die Deutsche Kreditwirtschaft (DK) zugelassenen Netzbetreiber ist der oben erwähnte B3S als Prüfgrundlage verwendet worden. Hingegen wurde bei Kreditinstituten nur selten eine Nachweisprüfung unter Verwendung des ergänzenden KRITIS-Moduls der BAIT durchgeführt.

Mehrstufiges Verfahren beim BSI

Im BSI durchlaufen die eingereichten Nachweise ein mehrstufiges Prüfverfahren. Zunächst prüft das BSI, ob die Nachweisunterlagen vollständig sind. Anschließend findet mindestens eine Plausibilitätsprüfung statt. Auf beiden Stufen ist in der Regel weitere Kommunikation mit den Betreibern Kritischer Infrastruktur erforderlich, da die Nachweise meist Defizite aufweisen und daher Informationen oder Dokumente nachgefordert werden müssen. So musste das BSI beispielsweise bei mehreren Nachweisprüfungen nachfragen, ob die Aspekte der besonderen Behandlung von Absicherungen Kritischer Infrastruktur in den Prüfungen behandelt worden waren. Anschließend hat das BSI entsprechend aktualisierte Sicherheitsleitlinien von Betreibern angefordert.

Um bei seinen Vollständigkeits- bzw. Plausibilitätsprüfungen nachvollziehen zu können, ob die Geltungsbereiche der Prüfungen bei den Betreibern Kritischer Infrastrukturen mit den registrierten Anlagen übereinstimmen, musste die Behörde ebenfalls mehrfach nachfragen und Betreiber um zusätzliche Unterlagen bitten. Auch fehlten häufig Details zur Prüfplanung und -durchführung.

Die von den Betreibern Kritischer Infrastrukturen beauftragten Prüfenden Stellen sollten den Betreibern jeweils bestätigen, dass diese – wie gefordert – angemessene Maßnahmen nach dem Stand der Technik umgesetzt haben. Dies war in den meisten Fällen nur mit teils erheblichen Einschränkungen möglich. Zur Dokumentation der festgestellten Defizite haben die Betreiber – wie vorgeschrieben – dem BSI Mängellisten mitgeliefert, in denen sie entsprechende Sicherheitsmängel (der Klassifikation „schwerwiegend" und/oder „gering") mitteilten. Bei schwerwiegenden Sicherheitsmängeln mussten die Betreiber zusätzlich eine Umsetzungsplanung mit Verantwortlichkeiten, sowie mit Maßnahmen und Zieldaten zur Behebung einreichen.

Bei mehreren Betreibern Kritischer Infrastrukturen im Zahlungsverkehr stellten die Prüfenden Stellen Sicherheitsmängel fest, deren Zahl überwiegend im einstelligen Bereich liegt. Dies gilt gleichermaßen für Banken wie für IT-Dienstleistern im Zahlungsverkehr. Einige der beaufsichtigten Institute müssen jedoch relativ viele solcher Sicherheitsmängel abstellen.

Die große Zahl der festgestellten Mängeln im Finanzwesen war überraschend, da viele Betreiber bereits seit längerem bereichsspezifischen Audits unterliegen und auch ihren Kunden ein funktionierendes Informationssicherheitsmanagementsystem belegen – etwa mit existierenden ISO-27001-Zertifikaten. Nach derzeitiger Sichtung der Mängel handelt es sich jedoch in vielen Fällen um grundlegende Defizite bei der Implementierung des nach § 8a Absatz 1 BSIG konformen Informationssicherheitsmanagements oder bei der Dokumentation, wie sie etwa im Umfeld von Zertifizierungsprüfungen ermittelt werden. Diese Mängel stellen in der Regel keine unmittelbare Gefahr für die Kontinuität des technischen und fachlichen Betriebs der Kritischen Infrastruktur dar.

5 Nächste Schritte und Fazit

Das BSI wird die von den Betreibern mitgeteilten Maßnahmen, die zur Behebung von Sicherheitsmängeln führen sollen, eng begleiten und auf deren Umsetzung hinwirken.

Im Einzelfall wird das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes[12] die Beseitigung von Sicherheitsmängeln gegebenenfalls mit anderer Zeitplanung und weiteren Maßnahmenbündeln verlangen. Schließlich kann das BSI im Rahmen der Nachweisprüfung zu dem Ergebnis kommen, dass eine detaillierte Tiefenprüfung bei einzelnen Betreibern Kritischer Infrastrukturen notwendig ist, und eine solche Prüfung vornehmen.

Den intensiven und konstruktiven Austausch zwischen Betreibern Kritischer Infrastrukturen und deren Verbänden einerseits und den Aufsichtsbehörden BSI und BaFin andererseits begrüßen beide – BSI und BaFin – ausdrücklich. Die vorliegenden Nachweise zur Erfüllung der Vorgaben des § 8a Absatz 1 BSIG belegen, dass die Thematik im Finanzwesen ernst genommen wird und angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozwessen getroffen wurden, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind. Sie zeigen jedoch auch, dass diese Arbeit die Beteiligten auch 2020 weiter beschäftigen muss, um festgestellte Mängel abzustellen, aber auch um die Widerstandsfähigkeit des Finanzwesens etwa bei anstehenden neuen Initiativen der Digitalisierung zu erhöhen.

12 Vgl. § 8a Absatz 3, Satz 4 BSIG.


© iStock/in-future

Cyberrisiken versichern

„Sicher“ im Namen

Autor

Dr. Frank Grund
Exekutivdirektor Versicherungs- und Pensionsfondsaufsicht, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

1 Wie sicher Versicherer selbst sind

1.1 Versicherer als Ziel von Cyberattacken

Wer das Wort „sicher“ im Namen führt, sollte selbst gegen alles Übel der Welt gewappnet sein – auch wenn es aus dem Cyberraum kommt.[1] Einen solchen Automatismus gibt es freilich nicht. Fakt ist jedenfalls: Versicherer sind – ähnlich wie Banken – beliebtes Ziel von Cyberangriffen. Der Grund liegt auf der Hand. Sie nehmen Gelder an und bewegen hohe Summen. Außerdem häufen sie riesige Mengen hochsensibler Daten an.

Wie viele Angriffe die Versicherer treffen, können wir derzeit nur vermuten. Was zum einen daran liegt, dass es bis dato, anders als bei Banken, keine Meldepflicht gibt, ein Manko, das dringend behoben werden sollte. Zum anderen dürfen wir annehmen, dass es unter den Hackern große Meister der Camouflage gibt. Wie viele gut getarnte Cyberangriffe unbemerkt von statten gehen, lässt sich daher kaum seriös schätzen.

Manche Hacker camouflieren zwar sich selbst, nicht aber ihre Angriffe. Sie legen es darauf an, dass ihre Taten auffallen, das macht ihre kriminelle Geschäftsidee aus. Beispiel Ransomware: Selbstverständlich sollen die Opfer erfahren, dass sie angegriffen worden sind. Es geht schließlich darum, für die Herausgabe ihrer Daten Lösegeld von ihnen zu erpressen.

Die Bedrohungslage ist ernst. Sie wird sogar zunehmend ernster, denn der Gegner wird immer besser. Die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (European Insurance and Occupational Pensions Authority – EIOPA) findet in ihrem Report „Cyber Risk for Insurers – Challenges and

1 Dieser Text basiert auf einer Rede, die der Verfasser am 21. Januar 2020 bei der Haftpflicht-Jahrestagung 2020 in Hamburg gehalten hat.

Opportunities“[2] aus dem Jahr 2019 deutliche Worte. Die zunehmende Häufigkeit und Raffinesse von Cyber-Attacken bereite Versicherern Schwierigkeiten. Anfällig mache sie der verstärkte Einsatz von Big Data und Cloud Computing. Hinzu kommt aber noch ein weiterer Aspekt, nämlich das drohende Konzentrationsrisiko.

1.2 Die eigene Abwehr stärken

Aber wie dem auch sei, die zentrale Frage lautet: Rüstet sich die Branche insgesamt ausreichend für den Kampf gegen Cyberkriminelle? Das sollte man annehmen, schließlich sind Kundendaten, auf die Kriminelle es absehen, der Schatz eines jeden Versicherers. Jedes Unternehmen dürfte daher aus eigenem Interesse ein Maximum an IT-Sicherheit anstreben.

Darauf wollen sich aber natürlich weder Gesetzgeber noch Aufsicht verlassen, und so gibt es regulatorische Vorgaben zur IT-Sicherheit und aufsichtliche Rundschreiben, die darauf aufsetzen. Unsere versicherungsaufsichtlichen Anforderungen an die IT haben wir in unseren gleichnamigen VAIT[3] zusammengefasst. Damit legen wir die Vorschriften des Versicherungsaufsichtsgesetzes (VAG) über die technisch-organisatorische Ausstattung der Unternehmen verbindlich und konsistent aus. Alle Unternehmen und Gruppen sollen wissen, woran sie sind. Diese Transparenz ist uns wichtig.

2 EIOPA, Cyber Risk for Insurers – Challenges and Opportunities, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf, abgerufen am 27.3.2020.

3 Rundschreiben 10/2018 – Versicherungsaufsichtliche Anforderungen an die IT (VAIT), www.bafin.de/dok/11102988.

Geplante Attacken im Namen der Sicherheit
In den VAIT verlangen wir unter anderem, dass der Informationssicherheitsbeauftragte in seinem Statusbericht an die Geschäftsleitung die Ergebnisse von Penetrationstests aufführt. Bei solchen Tests versucht ein Sicherheitsspezialist, die Leistungsfähigkeit der IT-Sicherheit eines Unternehmens zu prüfen. Neuere Varianten – wie etwa TIBER-Tests – konzentrieren sich nicht mehr überwiegend auf technische Aspekte, sondern berücksichtigen auch Faktoren wie menschliche Fehler. Bei solchen Red-Team-Tests versucht ein Red Team, wie reale Angreifer, die physischen, technischen oder organisatorischen Sicherheitsmechanismen eines Unternehmens zu überwinden, um vorher definierte Ziele zu erreichen.

Zu den Stärken von Red-Team-Tests zählen Realitätsnähe, Prüfungstiefe, Verwertbarkeit und Anschaulichkeit der Ergebnisse. Bei solchen geplanten Attacken werden die möglichen Auswirkungen eines Hacker-Angriffs demonstriert – und zwar auf anschauliche Weise, so dass sich auch Personen ein Bild von der Bedrohungslage machen können, die keine IT-Sicherheitsexperten sind. Konkrete Schwachstellen in den Sicherheitsmaßnahmen der Unternehmen werden offengelegt und – im Idealfall zügig – behoben. Solche Red-Team-Tests sind keine Pflichtübung, aber die Unternehmen sollten dieses Instrument aus eigenem Interesse nutzen, um ihre Cybersicherheit zu verbessern. Es wäre unsinnig, wenn die Versicherer bei nicht traumschönen Ergebnissen aufsichtliche Sanktionen befürchten müssten und deswegen auf die Tests verzichteten. Bei einem Red-Team-Test geht es nicht um Bestehen oder Nichtbestehen. Es geht einzig um ein Optimum an Cybersicherheit.

1.3 Offene Flanke

Die BaFin selbst führt keine Penetrationstests durch, aber eigene IT-Prüfungen. Die fördern mitunter überraschende Erkenntnisse zutage, die nicht durchweg positiv sind. Wir haben bei Prüfungen 2019 und 2020

festgestellt, dass mehrere Versicherer nicht einmal ein Informationsrisikomanagement eingerichtet hatten. Sie hatten sich weder systematisch und angemessen mit den wesentlichen Informationsrisiken auseinandergesetzt. Noch hatten sie die erforderlichen Elemente Identifikation, Bewertung, Überwachung und Steuerung aufgesetzt, wie es in den VAIT gefordert wird. Diese Unternehmen hatten eine offene Flanke, denn ohne ein wirksames Informationsrisikomanagement lassen sich Cybergefahren nun einmal nicht abwehren.

Beim Informationssicherheitsmanagement sieht es ähnlich aus: Bei manchen Unternehmen suchten wir es vergebens, oder es war nicht angemessen. Unsere Prüfer fragten nach Informationssicherheitsleitlinien oder auch nur nach dem Informationssicherheitsbeauftragten – in einigen Fällen leider vergeblich. Es kann auch nicht sein, dass manche Systeme und Applikationen gar nicht auf Sicherheitsvorfälle geprüft werden. Das alles sind eklatante Lücken.

Angesichts der Gesamtlage ist es denn auch nicht verwunderlich, dass die BaFin im Jahr 2020 schwerpunktmäßig die IT- und Cybersicherheit unter anderem von Versicherungsunternehmen untersuchen will. Die Aufsicht will dazu vor allem kontrollieren, wie in der Branche die VAIT umgesetzt werden. Mit Blick auf die rasante Ausbreitung des Corona-Virus sind wir allerdings gezwungen, unsere Schwerpunkte für das Jahr 2020 anzupassen. Was auf der anderen Seite aber nicht heißt, dass wir die Augen vor IT- und Cyberrisiken verschließen, bis ein Impfstoff gefunden ist.

2 Cybervorfälle bei Dritten – ein Risiko für Versicherer

2.1 Versteckte Risiken

Jenseits des eigenen Risikos, Opfer von Cyberangriffen zu werden, müssen Versicherer gegebenenfalls Cybervorfälle bei Dritten decken. Ob ein Versicherungsunternehmen für Cyberrisiken Dritter geradestehen muss, hängt nicht davon ab, ob sich die Police „Cyberversicherung" nennt. Cyberrisiken können auch in Versicherungsprodukten schlummern, die – anders als Cyberpolicen – nicht ausdrücklich regeln, inwieweit Cyberschäden gedeckt sind. Man spricht hier von versteckten oder non-affirmativen Cyberrisiken beziehungsweise von silent cyber risks. Solche versteckten Risiken lauern in vielen traditionellen Verträgen. Einige dieser Verträge stammen aus einer Zeit, in der das Thema Digitalisierung/Cyberrisiko noch keine oder zumindest keine große Rolle spielte.

Betroffen sind vor allem Schaden- und Unfallversicherer. Die massive Zunahme von Hackerangriffen und anderer Formen von Cybervorfällen könnte vor allem bei ihnen zu disruptiven Schadenentwicklungen führen. Angenommen, ein Hacker schaltet das Kühlsystem einer Industrieanlage aus und entfacht damit einen Brand. Dann läge die versicherte Gefahr „Brand" vor, und der Sachversicherer müsste zahlen. Dass er in analogen Zeiten bei Vertragsschluss nicht an das Szenario „Hacker schaltet Kühlsystem aus" gedacht hat, möglicherweise auch gar nicht denken konnte, spielt hierbei keine Rolle.

Non-affirmative Cyberrisiken als Aufsichtsschwerpunkt 2019

Non-affirmative Risiken waren 2019 ein Schwerpunkt der Versicherungsaufsicht. Die BaFin wollte darauf hinwirken, dass Versicherer die non-affirmativen Cyber-Risiken im eigenen Versicherungsbestand identifizieren und bewerten. Dazu hat die Aufsicht ihre örtlichen Prüfungen genutzt, non-affirmative Cyberrisken waren aber auch Thema in Aufsichtsgesprächen.

Zusätzlich hat die BaFin 27 Versicherer bzw. Versicherungskonzerne zu non-affirmativen Cyberrisiken befragt, um sie für das Thema zu sensibilisieren. Nur zwei Unternehmen haben bislang angegeben, es seien Schäden durch non-affirmative Cyberrisiken in ihren Beständen entstanden. Auffällig war, dass viele Versicherer bis dato noch keine solchen Versicherungsfälle zu vermelden hatten. Das könnte man dahingehend interpretieren, dass die Branche die Gefahr non-affirmativer Cyberrisiken möglicherweise etwas überschätzt hat. Eine Entwarnung für alle Gesellschaften und jeden Bestand gibt unsere Abfrage aber nicht her – auch und vor allem, weil es uns noch an Daten fehlt. Rund 50 Prozent der Befragten gaben an, dass es nicht leicht sei, derartige Fälle überhaupt zu identifizieren.

Die gute Nachricht: Fast alle Versicherer berücksichtigten non-affirmative Risiken 2019 in ihrem Risikomanagement und beobachteten Schadenentwicklung und Marktgeschehen. Die Unternehmen haben auch damit begonnen, ihre Allgemeinen Versicherungsbedingungen mit Blick auf silent risks zu durchforsten. Umfangreichere Vertragsänderungen standen aber nicht zur Debatte.

Zusammenfassend zwei Botschaften: Versicherungsunternehmen müssen – erstens – intensiver als bislang prüfen, ob Cybervorfälle Ursache eines Schadens sind. Zweitens gilt gerade angesichts eventueller non-affirmativer Cyber-Risiken: Die Unternehmen müssen ihr Portfolio kennen – oder schnellstmöglich kennenlernen!

2.2 Cyberpolicen

Produkte, die sich Cyberversicherung nennen und Cyberrisken ausdrücklich versichern, sind relativ neu, aber es gibt sie seit einigen Jahren. Es mangelt auch nicht an Musterbedingungen des Gesamtverbandes der Deutschen Versicherungswirtschaft. Cyberversicherungen sind keine traditionellen Produkte. Sie gehören zu den wenigen Innovationen, welche die Digitalisierung im Versicherungssektor hervorgebracht hat. Und sie schließen eine Deckungslücke zwischen klassischen

Versicherungen – etwa zwischen einer Betriebsunterbrechungs- und einer Haftpflichtversicherung.

Wenn Angreifer das IT-System eines Betriebs lahmlegen und Kundendaten stehlen, ist dieser Betrieb bei seinem Betriebsunterbrechungs- und Haftpflichtversicherer meist an der falschen Adresse. Liegt kein Sach- oder Personenschaden vor, decken viele klassische Policen dieser Sparten weder den Ertragsausfall noch die Forderungen geschädigter Dritter, an deren Konten sich die Hacker bedient haben. Die Cyberversicherung soll solche Lücken schließen.

Wachstumsmarkt

Cyberversicherungen gelten als Wachstumstreiber. Das Wirtschaftsprüfungs- und Beratungsunternehmen KPMG hat das Prämienvolumen 2016 für Deutschland auf 100 Millionen US-Dollar beziffert.[4] Diese Zahl dürfte zwar mittlerweile gestiegen sein, angesichts des 2,9 Milliarden Dollar schweren US-Marktes aber immer noch bescheiden ausfallen. Und ja, es gibt in Europa noch einen Cyber-Gap, den der Markt schließen kann, wodurch er wüchse.

Wir sollten hier aber keine Apfel-mit-Birnen-Vergleiche anstellen. Der deutsche Markt ist grundlegend anders als der US-Markt, der sehr stark vom Rechtsschutzgedanken geprägt ist. Überzogene Wachstumsphantasien waren zudem noch nie hilfreich. Wie verlässlich sind Prognosen, wenn wir noch nicht einmal gesicherte Ist-Zahlen haben? Versicherungsunternehmen sind nicht verpflichtet, uns Aufsehern separate Zahlen zu Cyberpolicen zu liefern. Das verlangt weder die Versicherungsberichterstattungs-Verordnung noch Solvency II.

Einige Erkenntnisse zum europäischen Cyber-Markt finden sich in einem Bericht von EIOPA.[5] Danach fokussieren sich die Versicherer auf gewerbliche Kunden, nehmen aber auch Einzelpersonen in den Blick. Die wachsende Zahl von Cybervorfällen treibe das Bewusstsein für das Risiko und damit die Nachfrage nach passenden Versicherungslösungen voran. Ein weiteres Ergebnis: Wenn Versicherer ihren Versicherungsschutz bepreisten, nutzten sie qualitative Modelle häufiger als quantitative.

Soviel zum EIOPA-Bericht. Natürlich hat die BaFin den Anspruch, sich ein eigenes Bild vom deutschen Markt für Cyberversicherungen zu machen. 2020 wollen wir ihn – so unsere Planung aus der Vor-Corona-Zeit – schwerpunktmäßig untersuchen und dazu etwa 25 Versicherern einige Fragen stellen. Uns interessiert, wie viele Cyberpolicen sie im Bestand haben, wie hoch das Beitragsvolumen ist und wie hoch die Schäden sind. Uns interessiert aber auch, ob die Unternehmen in der Lage sind, Cyberrisiken richtig zu bepreisen. Deshalb wollen wir auch Erkenntnisse über das Underwriting und das Risikomanagement gewinnen.

Warten wir ab, wie weit wir in diesem Jahr angesichts der Corona-Krise mit diesen Plänen kommen. Aber auch in Zeiten der Pandemie gilt der ebenso bekannte wie dringliche Appell an die Versicherer: Cyberpolicen vorsichtig zeichnen, die Prämieneinnahmen nicht überschätzen und die Kumulrisiken nicht unterschätzen!

4 KPMG, Neues Denken, Neues Handeln – Insurance Thinking Ahead Versicherungen im Zeitalter von Digitalisierung und Cyber, Studienteil B: Cyber, Seite 7, https://assets.kpmg/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf, abgerufen am 6.4.2020.

5 EIOPA, Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf, abgerufen am 27.3.2020.

3 In eigener Sache: IT-Sicherheit der BaFin

Auch sich selbst verlangt die BaFin in Fragen der IT-Sicherheit sehr viel ab, denn sie ist ebenfalls ein beliebtes Ziel von Angreifern aus dem Cyberraum. Was nicht verwunderlich ist, wenn man zum Beispiel bedenkt, dass auch sie über eine Fülle an hochsensiblen Daten verfügt – darunter die, welche Versicherer, Banken und andere Finanzdienstleister ihr melden müssen.

Wie sich die BaFin schützt? An dieser Stelle nur einige Beispiele: Wie alle Bundesbehörden ist auch sie verpflichtet, die Empfehlungen zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umzusetzen. Darüber hinaus befolgt die BaFin die einschlägigen DIN-Normen und die Vorgaben der Europäischen Zentralbank (EZB). Hintergrund ist die Einbindung der BaFin in den Einheitlichen Aufsichtsmechanismus für die Banken der Eurozone unter Leitung der EZB.

Auch über die zentralen Absicherungsmaßnahmen des Netzes der Bundesverwaltung wird die BaFin geschützt. Zusätzlich wappnet die Aufsicht ihr Netzwerk aber mit eigenen Maßnahmen. Sie verfügt über ein umfassendes und fortlaufend aktualisiertes Sicherheitskonzept, das einen Angriff auf ihre IT-Infrastruktur extrem erschwert. Details macht die Behörde aus wohl nachvollziehbaren Gründen nicht öffentlich. Daher nur so viel: Alle Zugänge zum Internet werden mehrstufig überwacht. Heruntergeladene oder per E-Mail zugesandte Dateien werden in Detonation Chambers geladen und dort in einer separierten Umgebung geprüft. Zertifizierte Firewalls und eine ganze Reihe von Virenabwehrmechanismen verstehen sich von selbst.

Und selbstverständlich legt die BaFin sehr viel Wert darauf, dass all ihre Beschäftigten verantwortungsvoll mit Daten und Fragen der Cybersicherheit umgehen, etwa indem sie sie sensibilisiert und schult.

Ob die BaFin Cyberattacken standhalten kann, wird regelmäßig extern geprüft – etwa durch den Bundesrechnungshof, die EZB, eigens beauftragte Auditoren – und Penetrationstests. Bislang hat man der BaFin dabei immer ein hohes Sicherheitsniveau attestiert. Bislang war auch keiner der Cyberangriffe auf die BaFin erfolgreich, soweit wir das beurteilen können. Sicher muss auch die Versicherungsaufsicht sein. Sie darf sich nur nicht allzu sicher fühlen.

Cyberversicherung wird zum Krisenmanager

Autor

Dr. Christopher Lohmann
Vorstandsvorsitzender Gothaer Allgemeine AG

mit Melanie Schmitz, Frank Huy,
Oliver Schulze und Udo Wegerhoff,
Gothaer Allgemeine AG

1 Einleitung

Nahezu jedes Hotel arbeitet heutzutage mit einem Online-Buchungssystem, die meisten Handwerker führen eine elektronische Kundenkartei, und kein Krankenhaus funktioniert mehr ohne digitale Patientenakten. Diese neuen Technologien bringen allen Bereichen enormen Fortschritt: Sie beschleunigen und vereinfachen Prozesse, und Aufgaben lassen sich orts- und zeitunabhängig erledigen. Doch Unternehmen werden dadurch auch angreifbarer: Wer auf Digitalisierung setzt, ist potenziell gefährdet, Opfer von Cyberattacken zu werden. Bei dem Gedanken an Datenklau, Hackerangriff, Identitätsdiebstahl, Viren, Trojaner oder sogar Cybererpressung bekommen nicht nur Informatiker feuchte Hände. Doch vor den Folgen können sich Unternehmen und Verbraucher schützen: mit Cyberpolicen[1].

Auch für Versicherer dürfte der junge Markt der Cyberpolicen aktuell der spannendste Trend im Bereich der Firmenversicherung sein: Neue Produkte und ein noch übersichtliches Bewerberfeld aus deutschen und anglo-amerikanischen Anbietern bei sich ständig ändernden Bedrohungslagen und technischen Neuerungen. Wer sich als Versicherer jetzt zurücklehnt, droht langfristig auf der Strecke zu bleiben.

Das Kundenpotenzial für Cyberversicherungen ist für Anbieter riesig. Schließlich ist eine IT-Infrastruktur heute aus keinem Unternehmen mehr wegzudenken – unabhängig davon, ob es sich um einen Industriekonzern oder einen mittelständischen Betrieb handelt.

1 Zum Thema Cyberpolicen siehe auch Seite 73 ff.

2 Wie groß die Angst der Mittelständler vor Hackerangriffen ist

Während große Firmen finanzielle Mittel besitzen, sich mit modernen Lösungen und internen wie externen IT-Experten gegen Cyberattacken zu schützen, sieht es bei kleinen und mittelständischen Unternehmen (KMU) meist anders aus. Dabei ist die Sensibilisierung für das Thema auch bei ihnen durchaus vorhanden. Das belegt die KMU-Studie der Gothaer aus dem Jahr 2019[2], an der Vertreter von mehr als 1.000 KMU teilgenommen haben. Vor der Coronakrise belegte der Hackerangriff mit 43 Prozent unangefochten Platz eins bei den Risiken, die Unternehmensleiter am meisten fürchten – und ließ damit Einbrüche (36 Prozent) und den Betriebsausfall (35 Prozent) hinter sich. Außerdem ergab die KMU-Studie, dass nahezu jedes fünfte befragte Unternehmen (17 Prozent) bereits Opfer eines Cyberangriffs geworden ist. Die Dunkelziffer dürfte deutlich höher sein, da Unternehmer nicht jede Attacke bemerken oder melden. Am häufigsten betroffen waren mittelständische Unternehmen mit 200 bis 500 Mitarbeitern, die in Deutschland oft Technologieführer in ihrem Bereich und daher ein besonders attraktives Ziel für Angreifer sind.

Das Risiko ist Unternehmern also bekannt. Sie fürchten sich nicht zu Unrecht vor den finanziellen und rechtlichen Folgen von Cyberkriminalität, die erheblich sein und in extremen Fällen bis zur existenziellen Gefährdung des Unternehmens reichen können. Zum Beispiel dann, wenn es zu einer lang anhaltenden Betriebsunterbrechung kommt. Daher ist es umso erstaunlicher, dass gerade Unternehmer die Absicherung dieser Risiken durch eine Cyberversicherung noch verhältnismäßig selten nutzen. In der KMU-Studie der Gothaer gaben nur 13 Prozent der Befragten an, eine Cyberpolice zu besitzen. Immerhin versicherten 23 Prozent aller befragten KMU, in den kommenden zwei Jahren solch einen Schutz abschließen zu wollen. Aber immer noch 41 Prozent planten es nicht, 36 Prozent waren unentschlossen.

Eines ist doch verwunderlich: Kaum ein Unternehmer verzichtet auf eine Betriebshaftpflicht: 88 Prozent der befragten KMU gaben in der Studie der Gothaer solch einen Vertrag an. Doch wenn ein Hackerangriff derzeit offenbar ihre größte Sorge ist, warum sichern sich immer noch so wenige Firmen mit einer Cyberversicherung gegen die finanziellen und rechtlichen Folgen eines solchen Zwischenfalls ab?

2 Gothaer, KMU-Studie 2019, https://www.gothaer.de/ueber-uns/presse/publikationen/studien/kmu-studie-2019.htm, abgerufen am 20.3.2020.

3 Schaden, ohne dass der Täter je die Firma betreten hat

Ganz langsam setzt ein Umdenken ein. Die Gothaer sieht das an ihren Abschlusszahlen: Im Jahr 2019 verzeichnete sie einen erheblichen Zuwachs an Cyberabschlüssen im Vergleich zum Vorjahr. Wachstumstreiber sind vor allem ein gesteigertes Risikobewusstsein bei den Unternehmensleitern, aber auch die Tatsache, dass im Versicherungsvertrieb die Bedeutung von Cyberversicherungen nach und nach steigt. Auch die zunehmende Medienberichterstattung über prominente Cyberattacken führt regelmäßig vor Augen, dass Firmen – unabhängig von Branche und Größe – ein lohnendes Ziel für Cyberkriminelle sind. Welche Risiken birgt dabei ein Hackangriff für Unternehmen? Die am weitesten verbreiteten Szenarien sind sicherlich der Datenklau und die Datenverschlüsselung. Im Jahr 2016 ist zum Beispiel das Klinikum Neuss Opfer eines Trojaners geworden, der alle nötigen Daten für den Krankenhausbetrieb verschlüsselte. Die Hacker legten das größte Krankenhaus der Stadt lahm, ohne je physisch einen Fuß hineingesetzt zu haben. Nichts ging mehr: Elektronische Patientenakten ließen sich nicht mehr öffnen, Medikamentendatenbanken waren nicht mehr abrufbar – und zum Schutz vor weiterer Ausbreitung schalteten Mitarbeiter fast alle Computer aus. Kurzum: Das Klinikum stand still. Und der Schaden, nachdem IT-Sicherheitsspezialisten jedes einzelne betroffene Computersystem säubern mussten, belief sich auf rund eine Million Euro.

Ähnliches kann auch einem kleinen Handwerksbetrieb oder einer Medienagentur passieren. Ein falscher Klick in den Anhang einer E-Mail, und die enthaltene Schadsoftware verbreitet sich im IT-Netzwerk, sperrt Zugänge und verschlüsselt Daten. Der Schaden liegt dann nicht nur beim Unternehmer, sondern möglicherweise auch beim Kunden, dessen Daten plötzlich nicht mehr sicher auf dem Firmenserver sind. Schlimmstenfalls breitet sich die Schadsoftware vom befallenen Computersystem zudem auf Dritte aus, was erhebliche Schadensersatzansprüche auslösen kann. Gerade ein solches Szenario sollte Selbstständigen zu denken geben: Cyberkriminalität bedroht nicht nur die Arbeitsprozesse und verursacht erhebliche finanzielle Schäden im eigenen Unternehmen – sie greift in manchen Fällen auch die Daten Dritter ab, für die das Unternehmen verantwortlich ist, oder richtet bei anderen einen Schaden an. Richtiges und schnelles Handeln zur Schadensbegrenzung und -behebung im Ernstfall ist somit Pflicht.

4 Wie Cyberversicherungen helfen

Der größte Mehrwert von Cyberpolicen ist, dass es sich dabei um mehr als eine reine Versicherung handelt, die dem Kunden seine finanziellen Schäden ersetzt. Cyberversicherungen unterstützen ganzheitlich, bieten also Service-Leistungen präventiv vor und unmittelbar nach dem Schadeneintritt – wie ein Krisenmanager.

Die Versicherung greift, vereinfacht gesagt, wenn sich der Versicherungsnehmer einem Hackerangriff ausgesetzt sieht oder ihm Daten gestohlen wurden. Die mitunter existenzbedrohenden Kosten der Wiederherstellung von Daten und Programmen übernimmt dann die Versicherung. Abgesichert sind sowohl Eigen- als auch Drittschäden des Versicherungsnehmers. Enthalten im Deckungskonzept der Gothaer sind zudem Ausgaben für einen nötigen Hardware-Austausch oder Betriebsunterbrechungskosten, auch bei vorsorglicher Systemabschaltung. Zusätzlich reguliert die Gothaer mögliche Schäden an Fertigungserzeugnissen durch den Hackangriff, sollte der Versicherungsnehmer ein Produktionsbetrieb sein.

5 Unterstützung im Krisenfall

Die Cyberversicherung kann auch für kleinere Unternehmen eine Unterstützung sein. Denn während große Konzerne im Versicherungsfall in erster Linie ihre Ausfälle ersetzt haben möchten, brauchen KMU ohne eigene IT-Abteilung und nötige Expertise mehr Hilfe. Eine gute Cyberpolice springt im Krisenfall als Manager ein. Dabei beginnt die Unterstützung mit einer 24/7/365 verfügbaren Hotline, über die Kunden Assistenz-Leistungen im IT-Security-Schadenfall rund um die Uhr erhalten und mögliche Angriffe melden können.

Ein Cyberangriff ist vor allem eines: zeitkritisch. Deshalb reguliert die Gothaer alle Kosten, die in den ersten 48 Stunden nach Schadenmeldung für die eingeschalteten IT-Sicherheitsexperten entstehen, immer – auch wenn sich später herausstellt, dass es keinen Hackerangriff gegeben hat. Auch bevor irgendetwas passiert, sollte ein umsichtiger Cyberversicherer Kunden wichtige Assistenz-Leistungen bieten. Die Gothaer unterstützt ihre Kunden etwa mit Schwachstellen-Scans und zeigt bei Bedarf IT-Sicherheitslücken auf, bevor Hacker sie ausnutzen können. Auch die Sensibilisierung der Belegschaft ist Teil des Produkts. Im Kern orchestrieren Versicherer über ihre Cyberpolicen das, was als Ökosystem und damit als Zukunft von Versicherungsschutz diskutiert wird.

6 Der Weg zum neuen Cyberprodukt

Ein Versicherer, der ein State-of-the-Art-Produkt anbieten möchte, sollte seinen Kunden neben der ständig verfügbaren Hotline also auch selbst mit Fachwissen zur Seite stehen. Bis die Gothaer an diesem Punkt war, musste sie selbst erst zur Expertin werden. Für die Versicherer, die heute mit einem ernstzunehmenden Cyberprodukt am Markt sind, war der Weg dorthin eine der spannendsten Herausforderungen der vergangenen Jahre. Wir mussten uns fragen: Welche Risiken gibt es überhaupt und welche Schäden in welcher Größenordnung können sie verursachen? Was können, wollen und was müssen wir absichern? Und welche Schutzmaßnahmen setzen wir bei unseren Kunden voraus? Um einen Überblick zu bekommen, war also zunächst viel Recherche nötig. Der Schlüssel für das richtige Pricing waren etwa Schadensszenarien, die wir für unterschiedliche Kundengruppen annahmen. Anhand dieser beispielhaften Schadenfälle schätzten wir Kosten ab und stellten für jedes einzelne Szenario nötige Versicherungsleistungen zusammen.

Eine große Herausforderung im Cyberbereich: Die Entwicklung und Vielfalt der Risiken sind ungebremst hoch und ständig im Fluss. Während sich etwa im Bereich Gebäudeversicherung eher wenig verändert, gleichen Cyberrisiken dem sich windenden, glitschigen Aal, den man mit einem möglichst großen Netz zu fangen versucht. Hier ist unsere Arbeit nicht mit der Produktentwicklung getan. Um unseren Schutz auch während der Vertragslaufzeit auf aktuellem Stand zu halten, sind pausenloses Monitoring und Agilität in der Produktentwicklung wichtig: Was sind aktuelle Gefahrentrends, wohin entwickeln sich Technik und Risiken, und muss das Versicherungsprodukt deswegen angepasst werden? Auf Seite der Kunden haben etwa ein Schreinermeister oder ein niedergelassener Arzt wenig Lust, sich neben der täglichen Arbeit auch noch mit den jeweils aktuellen Bedrohungen der Cyberkriminalität auseinanderzusetzen. Möglicherweise birgt das eine große Chance für Versicherer: Sie nehmen den Kunden diese Recherche ab und stehen ihnen zur Seite – ohne dabei deren individuellen Schutzstatus aus dem Blick zu lassen. Neben der Cyberpolice müssen Versicherungsnehmer schließlich auch selber zur IT-Sicherheit seines Unternehmens beitragen.

Eine weitere Aufgabe in der Cyberproduktentwicklung war neben der Beobachtung von Bedrohungsszenarien die hohe versicherungstechnische Komplexität. Cyberschäden als klassisches Kumulrisiko[3] betreffen eine Vielzahl von Sparten, streifen etwa die Haftpflicht-, Betriebsunterbrechungs-, Rechtschutz- und D&O-Versicherung[4] sowie die Technische Versicherung und die Elektronik- oder auch Vertrauensschadenversicherung. Die Gothaer musste Komponenten all dieser Einzelversicherungen sinnvoll in einem Produkt zusammenziehen, hauptsächlich bezogen auf Vermögensschäden. Schon in der frühen Phase der Produktentwicklung war es wichtig, auch mögliche spätere Implikationen, etwa andere Versicherungssparten, die von Cyberrisiken bedroht sein könnten, im Blick zu halten[5].

3 Unter Kumulrisiko versteht man das Risiko eines Versicherers, dass durch den Eintritt ein und desselben zufälligen Ereignisses gleichzeitig bei mehreren oder vielen versicherten Einheiten Schäden ausgelöst werden.

4 D&O steht für Directors-and-Officers.

5 Zum Silent-Cyber-Thema vgl. auch Seite 73.

7 IT-Sicherheit fällt nicht vom Himmel: Nachweispflichten

Eine Hausratversicherung erhält niemand, der seine Wohnungstür nicht abschließen kann oder gar keine hat. Gleiches gilt für eine Cyberversicherung: Abschlussvoraussetzung bleibt ein Mindestmaß an eigenen Sicherheitsvorkehrungen des Versicherungsnehmers. Unternehmer müssen unter anderem auf allen Computern einen Virenschutz installieren, Geschäftsdaten mit beschränkten Nutzerzugängen vor Unbefugten abschirmen und regelmäßig sichern. Schließlich dürfen sie eines nicht unterschätzen: Der größte Risikofaktor sitzt – salopp gesagt – immer noch vor dem Bildschirm: der Mensch. Die beste Firewall kann nicht schützen, wenn Mitarbeiter ahnungslos auf jeden E-Mail-Link klicken oder unsichere Passwörter benutzen. Deshalb ist es auch an den Unternehmen, ihre Belegschaft für Cyberrisiken zu sensibilisieren. Zugleich müssen Nutzer ermutigt werden, beim Verdacht auf einen Hackerangriff umgehend davon zu berichten, statt aus Verlegenheit zu schweigen, während sich ein potenzieller Schaden ausbreitet.

8 Welches Schutzniveau Versicherungskunden brauchen

Cyberinteressierte Versicherungskunden sollten, wie gesagt, ein Mindestmaß an Sicherheitsvorkehrungen vorhalten – was übrigens nicht nur im Interesse der Versicherung liegt, sondern auch im vitalen Eigeninteresse des Versicherungsnehmers. Keinesfalls lassen sich dabei alle Kundengruppen über einen Kamm scheren. Der Handwerker als Gewerbekunde benötigt eine andere IT-Umgebung und somit einen anderen Schutzstatus als ein mittelständisches Produktionsunternehmen. Trotzdem benötigen beide eine Cyberversicherung.

Daher geben wir als Gothaer unseren Gewerbekunden einen Katalog von fünf technischen Obliegenheiten an die Hand, die sie erfüllen müssen. Dazu gehören unter anderem ein Antivirenprogramm und eine Firewall. Im Industriebereich hingegen muss sich der Versicherungsnehmer hinsichtlich der IT-Sicherheit an den allgemein anerkannten Regeln der Technik orientieren. Daneben gibt es in der täglichen Praxis noch eine Vielzahl von Standards und Normen, die uns teilweise von den Versicherungsnehmern im Risiko-Assessment nachgewiesen werden. Beispiele sind die Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) als Bestandteile der IT-Grundschutz-Methodik oder die international gebräuchliche und in der Praxis beliebte ISO/IEC Norm 27001.

9 Wie Cyberversicherungen Standards setzen

Cyberpolicen haben das Potenzial, Maßstäbe zu setzen. Voraussetzung dafür ist allerdings, dass sich im Cyberversicherungsmarkt künftig einheitliche Standards für Sicherheitsmaßnahmen etablieren, die Versicherungsnehmer derzeit fordern. Dabei müssen stets auch die wettbewerbs- und kartellrechtlichen Restriktionen berücksichtigt werden. Momentan gleicht dieser Markt noch eher einem Flickenteppich. Denn jeder Versicherer erwartet Unterschiedliches von den Kunden. Fragt der eine Versicherer per Fragebogen nur rudimentäre Anforderungen ab, verlangt der andere in einem langen Katalog detaillierte Obliegenheiten. Würde der Markt hier einheitliche Grundstandards entwickeln, die von allen Cyberversicherungskunden vorgehalten werden müssten, hätte dies sicherlich positive Auswirkungen auf die gesamtgesellschaftliche Cybersicherheit.

Auch was die Instrumente betrifft, die Versicherer bei der Risikoanalyse und bei der Schadenregulierung einsetzen, bietet sich am Cyberversicherungsmarkt ein uneinheitliches Bild. Hier gilt abermals: Eine Vereinheitlichung könnte Standards schaffen, die zu mehr IT-Sicherheit in der Breite führen.

Die Kehrseite der Medaille: Die Vereinheitlichung von geforderten Sicherheitsmaßnahmen und angebotenen Dienstleistungen könnte den Wettbewerb schwächen. Denn gerade über das Angebot von sehr unterschiedlichen Prozessen, Dienstleistungen und Instrumenten lassen sich möglicherweise vorteilhafte Positionen in diesem jungen Markt einnehmen – und somit Kunden gewinnen und halten. Wir sehen: Bei der Cyberversicherung ist noch vieles im Fluss und niemand weiß, wie das Gesamtfeld der Versicherer und ihr Angebotsspektrum in einigen Jahren aussehen wird.

10 Chancen und Risiken von Cyberversicherern

Cyberpolicen sind für Versicherungsunternehmen sowohl Chance, als auch Herausforderung und Risiko. Positiv für Versicherer ist die seltene Möglichkeit, ein Produkt in einem ungesättigten Markt anbieten zu können, ohne dabei einem reinen Verdrängungswettbewerb ausgesetzt zu sein. Zusätzlich ist mit einem überdurchschnittlichen Wachstum auf der Beitragsseite zu rechnen. Eine Prognose, die in den vergangenen Jahren von einem namhaften Beratungsunternehmen erstellt wurde, geht in den nächsten 20 Jahren sogar von erreichbaren Beitragsgrößenordnungen von zweistelligen Milliardenbeträgen für die DACH-Region[6] aus. Aber auch wenn solche Größenordnungen nicht erreicht werden sollten, ist dieses Segment derzeit die Versicherungssparte mit der größten Wachstumsprognose.

Das Riskante: Im Gegensatz zu etablierten Sparten stehen für Cyberversicherungen derzeit kaum belastbare aktuelle oder vergangene Daten zur Verfügung. Das macht die Risikobewertung, -modellierung und Schadeneinschätzung versicherungstechnisch anspruchsvoll. Die Erfahrungswerte, die zur Verfügung stehen, stammen zudem meist aus anglo-amerikanischen Märkten und sind nur begrenzt auf den deutschen Markt übertragbar. Ein weiterer erschwerender Faktor ist die Tatsache, dass es sich um eine Sparte mit Risiken handelt, die einem sehr schnellen und großen Änderungsrisiko unterliegt, was die Bedrohungslage und die technologische Entwicklung betrifft. Daraus resultiert, dass die zu erwartenden Schäden sowohl in ihrer Quantität als auch in ihrer Qualität nur mit einer begrenzten Bestimmtheit in die Betrachtung und Bewertung aufgenommen werden können. Getroffene Annahmen und Szenarien sind somit einem permanenten Monitoring zu unterziehen, um diese dann validieren und anpassen zu können.

6 Die DACH-Region umfasst die Länder Deutschland, Österreich und Schweiz.

11 Fazit: Unterstützung durch das Ökosystem

Um mögliche Auswirkungen von Cyberschäden für Versicherungsunternehmen in einem vertretbaren Rahmen zu halten – gerade im Hinblick auf die schmale Datenbasis und die sich stetig ändernde Bedrohungslage –, sind neben einem permanenten Monitoring und Abgleich getroffener Annahmen, Szenarien und Parameter auch alle bekannten versicherungstechnischen Optionen zu nutzen. Dazu gehören ein vertretbarer Bedingungsrahmen, ein behutsamer Umgang mit Kapazitäten und der Einsatz von Sublimitierungen bei schwer kalkulierbaren Deckungserweiterungen.

Zudem setzen einige Versicherer – so auch die Gothaer – verstärkt auf die Unterstützung von Präven-

tionsmaßnahmen durch spezialisierte Dienstleister. Das Ökosystem Cyber, also das Zusammenwirken von Versicherungsunternehmen mit spezialisierten IT-Sicherheitsdienstleistern als Unterstützung bei der Risikoanalyse, Schadenbewertung oder Risikoprävention, wird somit immer ausgeprägter und elementarer für eine langfristig positive Ausgestaltung der Cyberversicherung. Zusätzlich besteht bei Versicherungsnehmern, zumindest bei kleineren und mittleren Unternehmen, ein Bedarf an IT-Sicherheitsunterstützung und Präventionsmaßnahmen, die das Ökosystem Cyber zu einem großen Teil bieten kann. Eine Win-Win-Situation für alle Beteiligten.

Impressum

Herausgeber
Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Gruppe Kommunikation
Graurheindorfer Straße 108 | 53117 Bonn
Marie-Curie-Straße 24 – 28 | 60439 Frankfurt am Main
www.bafin.de

Redaktion und Layout
Referat Öffentlichkeitsarbeit und Reden
Redaktion:
Annkathrin Frind
Tel.: +49 (0)228 4108-7776
Ursula Mayer-Wanders
Tel.: +49 (0)228 4108-2978
Jens Valentin
Tel.: +49 (0)228 4108-2363

E-Mail: perspektiven@bafin.de

Designkonzept
werksfarbe.com | konzept + design
Humboldtstraße 18, 60318 Frankfurt
www.werksfarbe.com

Bonn und Frankfurt am Main | 11. Mai 2020
ISSN 2625-5952

Bezug
Die Schriftenreihe BaFinPerspektiven erscheint auf der Internetseite der BaFin jeweils in deutscher und englischer Sprache. Die englische Ausgabe erscheint unter dem Titel „BaFinPerspectives“. Mit dem Abonnement des Newsletters der BaFin werden Sie über das Erscheinen einer neuen Ausgabe per E-Mail informiert. Den BaFin-Newsletter finden Sie unter:
www.bafin.de » Newsletter.

Satz
Mumbeck - Agentur für Werbung GmbH
Schlieffenstraße 60
42329 Wuppertal

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
60386 Frankfurt am Main

Bundesanstalt für
Finanzdienstleistungsaufsicht (BaFin)
Gruppe Kommunikation
Graurheindorfer Straße 108, 53117 Bonn
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main
www.bafin.de