BaFin Bundesanstalt für Finanzdienstleistungsaufsicht

Publikationen & Daten

© In-future/iStockphoto.com / BaFin

25.05.2020

BaFinPerspektiven 1 | 2020

Aufsicht über Informationssicherheit und Cloud-Computing verlangt europaweite Harmonisierung

Inhalt

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.

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) 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[3] anschließende „Consultation on a new digital finance strategy for Europe / FinTech action plan“ 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.

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. Nichtöffentliche 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.

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.

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.

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 Informationssicherheitsmanagement, 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 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 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.

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.

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 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 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.

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.

Autorinnen
Silke Brüggemann
Referentin, Referat Grundsatz ITAufsicht und Prüfungswesen
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Sibel Kocatepe, Referentin
Referat Grundsatz ITAufsicht und Prüfungswesen
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

Fußnoten:

1 EU-Kommission, FinTech-Aktionsplan: Für einen wettbewerbsfähigen und innovativeren [https://ec.europa.eu/transparency/regdoc/rep/1/2018/DE/COM-2018-109-F1-DE-MAIN-PART-1.PDF] 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; siehe dazu auch Infokasten "FinTech-Aktionsplan".

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 06.05.2020.

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 21.04.2020.

4 FSB, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices [https://www.fsb.org/wp-content/uploads/P131017-2.pdf] ,abgerufen am 12.01.2020.

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.
8 Vgl. BaFinJournal Januar 2018, und BaFinPerspektiven "Cyberkriminelle sind relativ faul" und BaFin, Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT), abgerufen am 6.5.2020.
9 Vgl. BaFinJournal April 2018, Seite 24 ff. und BaFin, Rundschreiben 10/2018 – Versicherungsaufsichtliche Anforderungen an die IT (VAIT), abgerufen am 6.5.2020.
10 BaFin, Rundschreiben 11/2019 (WA) – Kapitalverwaltungsaufsichtliche Anforderungen an die IT (KAIT) vom 1.10.2019, abgerufen am 6.05.2020.
11 Vgl. Aufsichtsschwerpunkte derBaFin 2020, Seite 9, abgerufen am 6.5.2020 .
12 a.a.O. (Fn. 1).
13 Joint Committee – European Supervisory Authorities, Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements [https://www.eiopa.europa.eu/sites/default/files/press/news/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf?source=search] - JC 2019 26,abgerufen am 10.3.2020.
14 Vgl. BaFinJournal April 2019, Seite 26 ff.
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/2017-esas-operations-consultation-document_en.pdf] , abgerufen am 7.1.2020.
18 a.a.O. (Fn. 3).
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 , abgerufen am 10.3.2020.
21 EBA, Press release: [https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/F EBA publishes guidelines on ICT and security risk management [https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/F , abgerufen am 06.05.2020.
22 a.a.O. (Fn. 21), Seite 6.
23 EIOPA, Consultation paper on the proposal for Guidelines on Information and Communication Technology ([http://https://www.eiopa.europa.eu/sites/default/files/publications/consultations/guidelines_ict_security_and_governance_12122019_for_consultation.pdf] ICT) security and governance [http://https://www.eiopa.europa.eu/sites/default/files/publications/consultations/guidelines_ict_security_and_governance_12122019_for_consultation.pdf] , abgerufen am 06.05.2020.
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.
27 JC 2019 26, S. 4, 18.
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] , 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.
31 Das Committee of European Banking Supervisors war Teil des Lamfalussy-Verfahrens der Europäischen Union.
32 Vgl. BaFinJournal April 2018, Seite 29 ff. und das "Merkblatt - Orientierungshilfe zu Auslagerungen an Cloud-Anbieter".
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.

Zusatzinformationen

BaFinPerspektiven 1 | 2020 (Download)

Publikation
BaFinPerspektiven Ausgabe 1 | 2020 (PDF, 6MB, barrierefrei)

Hinweis

Nutzungsbedingungen
