EUROPÄISCHE ZENTRALBANK

BANKENAUFSICHT

Andrea Enria
Vorsitzender des Aufsichtsgremiums

Herrn Markus Herbrand
Mitglied des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Frankfurt am Main, 30 April 2021

Ihr Schreiben vom 26. März 2021

Sehr geehrter Herr Abgeordneter,

vielen Dank für Ihr Schreiben zu IT- und Cyberrisiken, das mir von Herrn Dr. Schäuble, dem Präsidenten des Deutschen Bundestages, mit einem Anschreiben vom 29. März 2021 übermittelt wurde. Einige Ihrer Fragen beziehen sich auf Finanzmarktinfrastrukturen (FMIs). Diese Fragen kann ich nur im Hinblick auf FMIs mit Bankzulassung beantworten, da nur diese in den Zuständigkeitsbereich der EZB-Bankenaufsicht fallen.

Seit Gründung der europäischen Bankenaufsicht zählen Cyberrisiken zu den Aufsichtsprioritäten. Laut der SSM-Risikomatrix für 2021[1] gehören Cyberkriminalität und IT-Störungen zu den wesentlichen Risiken, denen beaufsichtigte Institute ausgesetzt sind. Bei vielen Instituten gibt es weiterhin Schwachstellen bei grundlegenden Cybersicherheitsprotokollen. Zudem ist die Architektur der Informations- und Kommunikationstechnologie (IKT) komplex, und eine steigende Anzahl von IKT-Systemen ist am Ende ihres Lebenszyklus angelangt. All dies muss noch in Angriff genommen werden. Im Bereich der IT- und Cyberrisiken stehen deutsche Banken vor recht ähnlichen Herausforderungen wie alle anderen Banken in der Bankenunion.

Die EZB-Bankenaufsicht führt etliche Tätigkeiten durch, um die IT- und Cyberrisiken, denen Banken ausgesetzt sind, zu überwachen und anzugehen. Erstens verfügt die EZB-Bankenaufsicht über ein Meldesystem für IT-Sicherheitsvorfälle: Alle von der EZB beaufsichtigten Banken sind verpflichtet, schwerwiegende Cyber-Sicherheitsvorfälle auf vertraulicher Basis zu melden, sobald diese erkannt wurden. So können die Aufseherinnen und Aufseher Trends erkennen und beobachten. Zudem können sie zeitnah reagieren, wenn ein größerer Cyber-Sicherheitsvorfall eine oder mehrere bedeutende Banken betrifft. Zweitens untersucht die EZB-Bankenaufsicht IT-Risiken in allen bedeutenden Instituten alljährlich im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (Supervisory Review and Evaluation Process – SREP). Drittens bieten häufige Vor-Ort-Prüfungen bei bedeutenden Instituten der EZB-

[1] EZB-Bankenaufsicht: Bewertung von Risiken und Schwachstellen für 2021.

Europäische Zentralbank
60640 Frankfurt am Main
Tel.: +49 69 1344 0
E-Mail: info@ecb.europa.eu
Website: www.bankingsupervision.europa.eu

Bankenaufsicht die Möglichkeit, die Kapazitäten einzelner Banken zur Steuerung von IT- und Cyberrisiken zu beurteilen.

In diesem Zusammenhang möchte ich auch auf den Jahresbericht über die Ergebnisse des SREP-Fragebogens zu IT-Risiken verweisen, den wir im Juli 2020 veröffentlicht haben.[2] In dem Bericht werden die wichtigsten Feststellungen zum Umgang der Banken mit IT-Risiken im ersten Quartal 2019 aufgezeigt. Die Outsourcing-Budgets der Banken stiegen im Laufe des Jahres 2018 und bis Anfang 2019 weiter an, wobei die Bedeutung von Cloud-Diensten zunahm. Thematisiert werden im Bericht auch unsere aufsichtlichen Bedenken angesichts der Anzahl an Systemen, die das Ende ihres Lebenszyklus erreicht haben, aber weiterhin kritische Geschäftsprozesse unterstützen. Der Bericht kommt auch zu dem Ergebnis, dass das Datenqualitätsmanagement weiterhin der schwächste Bereich der Risikokontrolle ist.

Die Aufsichtstätigkeiten der EZB orientieren sich an den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, die seit dem 30. Juni 2020 gelten. Darin ist beschrieben, wie alle Finanzinstitute die internen und externen IKT- und Sicherheitsrisiken, denen sie ausgesetzt sind, steuern sollten. Mit Blick auf die Zukunft ist der Vorschlag der Europäischen Kommission für einen Rechtsakt zur digitalen Betriebsstabilität (Digital Operational Resilience Act – DORA) eine begrüßenswerte Initiative. Ziel ist es, bestehende Regelungen zur Steuerung von IKT-Risiken und zur Meldung IKT-relevanter Sicherheitsvorfälle zu harmonisieren und zu straffen. Zudem sollen neue Regeln für ethisches Hacking auf der Basis von Bedrohungsinformationen und zur Steuerung von IKT-Risiken, die von Dritten ausgehen, eingeführt werden.

Der Ausbruch der Corona-Pandemie (Covid-19) hat sich auch auf IT- und Cyberrisiken ausgewirkt. Digitale Technologien waren zwar schon seit geraumer Zeit eine Herausforderung für die traditionellen Wertschöpfungsketten im Bankensektor. Durch die Pandemie wurde dieser Prozess aber kräftig beschleunigt. Sie hat deutlich gemacht, dass die Banken ausgereifte digitale Lösungen brauchen, um ihre Produkte und Dienstleistungen am Markt anbieten zu können. Dabei haben die unter die europäische Bankenaufsicht fallenden Banken gezeigt, dass sie operationell widerstandsfähig sind, selbst als immer mehr Mitarbeiter von zuhause arbeiteten. Die Banken haben ihr operatives Geschäft angepasst, um den Geschäftsbetrieb aufrechtzuerhalten. So waren sie in der Lage, ihre Leistungen auch weiterhin grenzüberschreitend anzubieten. Gleichzeitig hat die Pandemie die Banken vor zusätzliche Herausforderungen gestellt, denn nun verschob sich der Schwerpunkt von Cyberbedrohungen. Indem die Banken ihre Prozesse in Notfallumgebungen verlagern, haben sie nicht nur vermehrt mit Cyberrisiken zu kämpfen, auch die Risiken und Folgen von IT-Pannen nehmen zu. So müssen die IT-Systeme der Banken vor allem widerstandsfähig genug sein, um der aktuell starken Abhängigkeit von Telearbeit und Remote-Dienstleistungen standzuhalten. Die Angriffsfläche hat sich durch die intensivere Nutzung virtueller privater Netzwerke (VPNs) und mobiler Geräte, die mit privaten Internet-Zugangspunkten verbunden sind, leicht vergrößert. Deshalb ist es so wichtig, dass Banken wissen, mit welchen Methoden Cyberkriminelle ihre remote arbeitenden Mitarbeiter ins Visier nehmen. Denn dann können sie geeignete Maßnahmen ergreifen, um dieses Risiko zu mindern. Die Banken müssen ihre IT- und Cyberrisikostrategien kontinuierlich anpassen und sicherstellen, dass ihre Mitarbeiter die Risiken im Zusammenhang mit Telearbeitsregelungen kennen und entsprechend geschult sind. Die EZB hat dies bereits zu Beginn der Pandemie in ihrem Schreiben an

[2] Annual report on the outcome of the SREP IT Risk Questionnaire.

alle bedeutenden Institute[3] vom März 2020 betont. Sie hat dabei darauf hingewiesen, dass Banken die Risiken vermehrter Cyberbetrugsfälle in ihren Notfallplänen angehen müssen. Die EZB-Bankaufsicht verfolgt die Entwicklungen weiterhin im Rahmen der laufenden Aufsicht und überwacht sie durch regelmäßige Telefongespräche mit den Banken.

Was Ihre Fragen zur Anzahl der Cybervorfälle bei bedeutenden Instituten angeht, so möchte ich Sie auf die Financial Stability Review der EZB vom November 2020 verweisen. Sie enthält einige Statistiken zu dieser Thematik.[4] Die Anzahl der Cybervorfälle, die von bedeutenden Instituten gemeldet wurden, ist im Lauf der Zeit zwar gestiegen. Im dritten Quartal 2020 waren die Institute aber nicht stark betroffen. Die Anzahl der Cybervorfälle, die bedeutende Institute der EZB gemeldet haben, ist im dritten Quartal 2020 und im Vergleich zu 2019 etwas gestiegen.

Was Angriffe auf die EZB betrifft, so war sie ein einziges Mal Opfer eines erfolgreichen Cyberangriffs. Das war im August 2019. Der Vorfall betraf die extern gehostete Website des Banks‘ Integrated Reporting Dictionary (BIRD) der EZB. Die geschäftlichen Auswirkungen beschränkten sich auf die mögliche Exfiltration von E-Mail-Adressen der Abonnenten des Newsletters, der regelmäßig über diese Website herausgegeben wird. Die Täter konnten nicht identifiziert werden, und über den Vorfall wurde damals in einer Pressemitteilung[5] berichtet.

Mit freundlichen Grüßen

[unterschrift]

Andrea Enria

[3] Siehe Schreiben der EZB-Bankaufsicht an alle bedeutenden Institute vom 3. März 2020.

[4] Siehe EZB, Financial Stability Review, Frankfurt am Main, November 2020. Die Abbildung 3.9 gibt einen Überblick über die Entwicklung von Vorfällen, die 2019 und 2020 über das Meldesystem für IT-Sicherheitsvorfälle gemeldet wurden. Für 2020 sind sie zudem nach Art des Vorfalls aufgeschlüsselt.

[5] Siehe die Pressemitteilung der EZB „ECB shuts down compromised BIRD website“ vom 15. August 2019.