Die Aufmerksamkeit für IT-Risiken wächst

Geldhäuser investieren viel Energie, um ihre Daten und Systeme zu schützen. Doch die Gefahrenlage rechtfertigt weitere Bestrebungen der Regulierer, die Sicherheit im Interesse der Institute und Kunden europaweit voranzutreiben.

Anja Schulz

In deutschen Kreditinstituten schreitet die Digitalisierung in allen Bereichen stetig voran. Offensichtlich erfüllt der Einsatz digitaler und internetbasierter Technologien zum einen die Bedürfnisse der Kunden. Zum anderen begünstigt dieser aber auch effizientere und effektivere bankinterne Prozesse und kann die Umsetzung regulatorischer Anforderungen erleichtern. Die Digitalisierung ist somit ein wichtiger Baustein für die Zukunftsfähigkeit der deutschen Kreditwirtschaft. Auf die Digitalisierungsstrategien der einzelnen Institute werden die Aufsichtsbehörden im Rahmen ihrer Analysen der individuellen Geschäftsmodelle als Kernelement des aufsichtlichen Überwachungsprozesses, auch Supervisory Review and Evaluation Process oder SREP genannt, daher ein besonderes Augenmerk richten.

Indem Geldhäuser zunehmend komplexere oder internetbasierte IT-Systeme nutzen, steigt jedoch die Gefahr von Ausfällen und Cyberangriffen, die erhebliche Auswirkungen auf die Bereitstellung der Dienste wie Onlinebanking für Kundinnen und Kunden oder die Sicherheit von Daten haben können. Der öffentlichen Berichterstattung ist regelmäßig zu entnehmen, dass diese Gefahr real ist. Zudem besteht aktuell eine stark erhöhte Bedrohungslage durch Cyberattacken als Folge des Krieges in der Ukraine, vor der das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Ausschuss für Finanzstabilität (AFS) warnen. Der Ende Oktober veröffentlichte Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2022 gibt ein ausführliches Bild über die jüngsten Angriffsvarianten auf staatliche Institutionen, Privatpersonen und Unternehmen inklusive Kreditinstitute. Im Berichtszeitraum vom 1. Juni 2021 bis 31. Mai 2022 fanden demnach die meisten Attacken mit so genannter Ransomware statt. Ransomware ist ein Schadprogramm, das den Zugriff auf gespeicherte Daten und Systeme häufig durch eine Verschlüsselung verhindert. Die Angreifer fordern in der Regel einen hohen Geldbetrag für die Entschlüsselung.

Regulierer bemühen sich um Datensicherheit

Den Aufsichtsbehörden, etwa der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und der Deutschen Bundesbank, sind diese mit der zunehmenden Digitalisierung in den Instituten verbundenen Risiken bewusst. Bereits im November 2017 hat die BaFin die „Bankaufsichtlichen Anforderungen an die IT“, kurz BAIT, in Form des Rundschreibens 10/2017 veröffentlicht, das vor allem für die Bereiche IT-Ausstattung und -prozesse die Mindestanforderungen an das Risikomanagement (MaRisk) ergänzt oder konkretisiert. Im vergangenen Jahr wurden die BAIT zuletzt überarbeitet, um

Kompakt

- Mit jedem weiteren Digitalisierungsschritt steigt nicht nur der Komfort für Bankkunden, sondern wächst auch die Angriffsfläche der Dateninfrastruktur in den Instituten.
- Im sich verschärfenden Wettbewerb der Banken, Sparkassen und Fintechs ist es die Aufgabe der Aufseher und Regulierer, einheitliche Standards für Schutz und Sicherheit zu etablieren.
- Angesichts zunehmender Cyberbedrohungen schützen die regulatorischen Maßnahmen nicht nur die Geldhäuser, sondern auch ihre Kunden sowie die gesamte europäische Volkswirtschaft.

insbesondere die Leitlinien für das „Management von IKT- und Sicherheitsrisiken" der Europäischen Bankenaufsichtsbehörde EBA in die Aufsichtspraxis zu übernehmen.

In der Regulatorik hat sich mittlerweile der in den EBA-Leitlinien verwendete Begriff des Informations- und Kommunikationstechnologie-Risikos, kurz IKT-Risiko, durchgesetzt. Die EBA definiert IKT- und Sicherheitsrisiken als Verlustrisiken aufgrund einer Verletzung der Vertraulichkeit, des Verlustes der Integrität von Systemen und Daten, einer unzureichenden oder fehlenden Verfügbarkeit von Systemen und Daten beziehungsweise einer mangelnden Fähigkeit, die IT-Systeme in einem angemessenen Zeit- und Kostenrahmen bei sich verändernden Umgebungs- oder Geschäftsanforderungen anzupassen. Dieser Begriff ist sehr weit gefasst und schließt alle Risiken ein, unabhängig davon, ob sie aus unzulänglichen oder fehlerhaften internen Prozessen, aus externen Ereignissen wie Cyberangriffen oder mangelnder physischer Sicherheit resultieren. IKT- und Sicherheitsrisiken sind den in den MaRisk-Anforderungen als wesentlich eingestuften operationellen Risiken zugeordnet, für die angemessene Risikomess- und Risikosteuerungsverfahren in den Instituten vorhanden sein müssen.

Die BAIT sind, wie die MaRisk, in themenspezifische Module gegliedert und prinzipienbasiert. Dies soll den Instituten den Freiraum geben, die Vorgaben mit ihren individuell eingesetzten Technologien und Verfahren risikoorientiert zu erfüllen. Derzeit liegen die Schwerpunkte bei bankaufsichtlichen IT-Prüfungen oft auf der Umsetzung der beiden Module Informationsrisikomanagement und Informationssicherheitsmanagement. Wichtig ist hierbei, dass die Vorgaben dieser Module nicht nur für digitale Daten gelten, die EDV-Systeme speichern und verarbeiten, sondern für alle Informationen eines Instituts. Das schließt Daten auf Papier mit ein.

Zur Einhaltung der Informationssicherheit spielt insbesondere die nach den BAIT einzurichtende Stelle des oder der Informationssicherheitsbeauftragten (ISB) eine herausragende Rolle. Dieser Position sollte daher ausreichend und geschultes Fachpersonal zugewiesen werden. Zudem ist empfehlenswert, sie als tragende Rolle möglichst weit oben in der Organisationsstruktur anzusiedeln. Die große Bedeutung dieses Postens verdeutlicht die Erwartungshaltung der Aufseher. Nach BAIT, Textziffer 4.6, soll jedes Institut die ISB-Funktion grundsätzlich im eigenen Haus einrichten. Ein Auslagern ist nur für sehr kleine Institute unter bestimmten Voraussetzungen zulässig.

In einer Befragung im Rahmen des diesjährigen LSI-Stresstests durch die BaFin und die Deutsche Bundesbank gaben 1.299 als weniger bedeutend eingestufte Kreditinstitute (Less Significant Institutions oder LSI) und 17 Bausparkassen Auskunft zu IT-Vorfällen in 2021 sowie zu umgesetzten und geplanten Maßnahmen zur Reduzierung der Risiken. Demnach planen mehr als drei Viertel der Institute, die finanziellen Ressourcen zum Schutz vor IT-Risiken in den kommenden fünf Jahren zu erhöhen. Fast 80 Prozent haben bereits eine Versicherung gegen Cyberrisiken abgeschlossen, um eventuelle finanzielle Verluste zu reduzieren. Weitere acht Prozent planen, dies ebenfalls zu tun.

Nach gleichen Regeln spielen

Im Rahmen ihres im September 2020 vorgelegten Pakets zur Digitalisierung des Finanzsektors will die EU-Kommission die digitale operationelle Resilienz des gesamten europäischen Finanzsektors durch eine gleichnamige EU-Verordnung, den Digital Operational Resilience Act (DORA), stärken. Gleichzeitig beabsichtigt sie damit auch eine Harmonisierung der Vorgaben zum Umgang mit IKT-Risiken für die europäischen Kreditinstitute. Die Regeln in DORA sind teils strenger oder konkreter als die derzeit geltenden Vorgaben in den BAIT. Da DORA eine EU-Verordnung ist, muss sie zum festgelegten Zeitpunkt der Erstanwendung von allen europäischen Kreditinstituten eingehalten werden. Der Termin liegt voraussichtlich im ersten Quartal 2025. Dann überschreibt DORA die BAIT-Vorgaben.

Zu den weiteren Themenbereichen in DORA mit großer Relevanz für deutsche Institute zählen zum einen die Klassifikation und die Meldung von IKT-Schadensfällen. Zum anderen fordert die Verordnung die Einrichtung von risikobasierten Testprogrammen, um etwa die Wirksamkeit von Notfallplänen und vorgesehenen Maßnahmen zur Absicherung der digitalen Betriebsstabilität zu prüfen. Die EBA hat DORA in ihrem Arbeitsprogramm für 2023 priorisiert und beabsichtigt, verschiedene Papiere, so genannte Regulatory Technical Standards (RTS), Implementing Technical Standards (ITS) oder Leitlinien, zur weiteren Konkretisierung einzelner Vorschriften der Verordnung im kommenden Jahr vorzulegen. Dann kommen neben den schon geplanten Aufwendungen zur Verbesserung des IKT-Risikomanagements zusätzliche Arbeiten und Investitionen auf die deutschen Institute zu. Gleichwohl führt kein Weg daran vorbei, die mit der fortschreitenden Digitalisierung verbundenen Risiken durch geeignete und aufsichtlich konforme Maßnahmen zu reduzieren, damit ein Mehrwert für die Finanzindustrie und die gesamte Volkswirtschaft entsteht. ■


© HFM

Autorin
Prof. Dr. Anja Schulz
hat die Stiftungsprofessur für Bankenregulierung an der Hochschule für Finanzwirtschaft und Management (HFM) in Bonn inne.